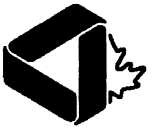
CMS Books in Mathematics

Alexander A. Mikhalev
Vladimir Shpilrain
Jie-Tai Yu

Combinatorial Methods

Free Groups, Polynomials, and Free Algebras

Canadian Mathematical Society
Société mathématique du Canada



Canadian Mathematical Society
Société mathématique du Canada

Editors-in-Chief
Rédacteurs-en-chef
Jonathan Borwein
Peter Borwein

Springer
Science+Business
Media, LLC

CMS Books in Mathematics
Ouvrages de mathématiques de la SMC

1 HERMAN/KUČERA/ŠIMŠA Equations and Inequalities

2 ARNOLD Abelian Groups and Representations of Finite Partially Ordered Sets

3 BORWEIN/LEWIS Convex Analysis and Nonlinear Optimization

4 LEVIN/LUBINSKY Orthogonal Polynomials for Exponential Weights

5 KANE Reflection Groups and Invariant Theory

6 PHILLIPS Two Millennia of Mathematics

7 DEUTSCH Best Approximation in Inner Product Spaces

8 FABIAN ET AL. Functional Analysis and Infinite-Dimensional Geometry

9 KŘÍŽEK/LUCA/SOMER 17 Lectures on Fermat Numbers

10 BORWEIN Computational Excursions in Analysis and Number Theory

11 REED/SALES (Editors) Recent Advances in Algorithms and Combinatorics

12 HERMAN/KUČERA/ŠIMŠA Counting and Configurations

13 NAZARETH Differentiable Optimization and Equation Solving

14 PHILLIPS Interpolation and Approximation by Polynomials

15 BEN-ISRAEL/GREVILLE Generalized Inverses, Second Edition

16 ZHAO Dynamical Systems in Population Biology

17 GÖPFERT ET AL. Variational Methods in Partially Ordered Spaces

18 AKIVIS/GOLDBERG Differential Geometry of Varieties with Degenerate Gauss Maps

19 MIKHALEV/SHPILRAIN/YU Combinatorial Methods

Alexander A. Mikhalev
Vladimir Shpilrain
Jie-Tai Yu

Combinatorial Methods

Free Groups, Polynomials, and Free Algebras

Springer

Alexander A. Mikhalev
Department of Mechanics
and Mathematics
Moscow State University
Moscow 119899
Russia
aamikh@cnit.math.msu.su

Vladimir Shpilrain
Department of Mathematics
The City College of New York
New York, NY 10031
USA
shpil@groups.sci.ccny.cuny.edu

Jie-Tai Yu
Department of Mathematics
The University of Hong Kong
Pokfulam Road
Hong Kong
China
yujt@hkusua.hku.hk

Editors-in-Chief
Rédacteurs-en-chef
Jonathan Borwein
Peter Borwein
Centre for Experimental and Constructive Mathematics
Department of Mathematics and Statistics
Simon Fraser University
Canada
cbs-editors@cms.math.ca

Mathematics Subject Classification (2000): 14-xx, 14Rxx, 17Bxx, 20Fxx

Library of Congress Cataloging-in-Publication Data
Shpilrain, Vladimir, 1960—
Combinatorial methods : free groups, polynomials, and free algebras / Vladimir Shpilrain, Alexander A. Mikhalev, Jie-Tai Yu.
p. cm. — (CMS books in mathematics series ; v. 19)
Includes bibliographical references and index.

1. Combinatorial group theory. 2. Lie algebras. 3. Polynomials. I. Mikhalev, Alexander A., 1965— II. Yu, Jie-Tai. III. Title. IV. CMS books in mathematics ; 19.
QA182.5.S57 2003
512'2—dc22 2003058951

ISBN 978-1-4419-2344-8 ISBN 978-0-387-21724-6 (eBook)
DOI 10.1007/978-0-387-21724-6

Printed on acid-free paper.

© 2004 SpringerScience+Business Media New York
Originally published by Springer-Verlag New York, Inc. in 2004
Softcover reprint of the hardcover 1st edition 2004
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (SpringerScience+Business Media New York), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden. The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

9 8 7 6 5 4 3 2 1 SPIN 10940891

Typesetting: Pages created by the authors using a Springer LaTeX 2e macro package.

www.springer-ny.com

To our parents

Preface

This book is about three seemingly independent areas of mathematics: combinatorial group theory, the theory of Lie algebras and affine algebraic geometry. Indeed, for many years these areas were being developed fairly independently. Combinatorial group theory, the oldest of the three, was born in the beginning of the 20th century as a branch of low-dimensional topology. Very soon, it became an important area of mathematics with its own powerful techniques.

In the 1950s, combinatorial group theory started to influence, rather substantially, the theory of Lie algebras; thus combinatorial theory of Lie algebras was shaped, although the origins of the theory can be traced back to the 1930s.

In the 1960s, B. Buchberger introduced what is now known as Gröbner bases. This marked the beginning of a new, "combinatorial", era in commutative algebra. It is not very likely that Buchberger was directly influenced by ideas from combinatorial group theory, but his famous algorithm bears resemblance to Nielsen's method, although in a more sophisticated form. More recently, in the 1990s, ideas from combinatorial group theory started to have a more direct and significant impact on the areas of commutative algebra and affine algebraic geometry through the work of several mathematicians including the authors of this book. It is remarkable that, also in the 1990s, ideas from algebraic geometry found their way into combinatorial group theory through the work of G. Baumslag, A. G. Myasnikov, V. Remeslennikov, O. Kharlampovich and B. I. Plotkin, thus creating a "two-way traffic" of ideas that allows algebraic geometry to shed light on group theory and vice versa.

The main purpose of this book is to show how ideas from combinatorial group theory have spread to the other two areas, with the main focus on the area of commutative algebra where the influence of these ideas has been especially spectacular.

We would like to emphasize that we only consider here purely combinatorial methods and results; in particular, we leave out important interactions of group theory with topology and geometry that were recently used with great success in solving several difficult problems about free groups and their automorphisms. We also leave out geometric methods in affine algebraic geometry and concentrate on combinatorial ones, in particular on those that come from combinatorial group theory.

The book is targeted at research mathematicians as well as graduate students with an interest in the general area of algebra.

Acknowledgments

It is a great pleasure for us to thank everyone who has directly or indirectly contributed to this book. Our special thanks go to E. I. Zelmanov for his everlasting support and encouragement. We are also grateful to V. A. Artamonov, V. Drensky, A. van den Essen, K. Q. Feng, L. Makar-Limanov, A. V. Mikhalev, U. U. Umirbaev, and A. A. Zolotykh for numerous helpful comments and insightful discussions. A. Pentus has helped us greatly in preparing a camera-ready copy of the manuscript.

We would also like to thank various institutions where all or some of us stayed or visited during the preparation of this book. First of all, the University of Hong Kong and its Institute of Mathematical Research brought together all three of us on several occasions. Our thanks also go personally to N. Mok, the Director of the Institute of Mathematical Research, M. K. Siu, the Chairman of the Department of Mathematics, and K. Y. Chan, the former Chairman of the Department of Mathematics, for their enthusiastic support of the algebraic program over many years. We are also grateful to our two other home institutions, Moscow State University and the City College of New York, for a stimulating research environment.

Finally, we are indebted to the staff of Springer-Verlag, in particular, to M. Spenser and Y.-S. Hwang, for their patience and help during the production process.

Moscow, Russia — Alexander A. Mikhalev
New York, NY, USA — Vladimir Shpilrain
Hong Kong — Jie-Tai Yu

Contents

Preface vii

Introduction 1

I Groups 5

Introduction 7

1 Classical Techniques of Combinatorial Group Theory 9
- 1.1 Nielsen's Method . . . 9
- 1.2 Whitehead's Method . . . 11
- 1.3 Tietze's Method . . . 13
- 1.4 Free Differential Calculus . . . 14
  - 1.4.1 Two applications . . . 17

2 Test Elements 20
- 2.1 Nielsen's Commutator Test . . . 21
- 2.2 Recognizing Test Elements . . . 25
- 2.3 Test Sets . . . 30
- 2.4 The "Double Jacobian" Matrix . . . 33

3 Other Special Elements 35
- 3.1 Δ-Primitive Elements . . . 35
- 3.2 Almost Primitive and Generic Elements . . . 41

4 Automorphic Orbits **45**
4.1 Finite Orbits 46
4.2 Abridged Orbits 48
4.2.1 Counting primitive elements 48
4.2.2 Complexity of Whitehead's algorithm 53
4.3 Endomorphisms that Preserve Automorphic Orbits . . . 59

II Polynomial Algebras **65**

Introduction **67**

5 The Jacobian Conjecture **71**
5.1 Polynomial Retracts and the Jacobian Conjecture 72
5.2 Retracts of $K[x, y]$ 75
5.3 Applications to the Jacobian Conjecture 76

6 The Cancellation Conjecture **80**
6.1 Equivalence and Stable Equivalence 83
6.2 Around Danielewski's Example 88

7 Nagata's Problem **92**
7.1 Gröbner Bases and Face Functions 95
7.2 Lifting the Nagata Automorphism 101

8 The Embedding Problem **108**
8.1 Embeddings of Curves in the Plane 109
8.1.1 Elementary automorphisms and peak reduction . 111
8.1.2 A classification of parametric curves 113
8.1.3 Embeddings of curves in the plane 115
8.2 Embeddings of Hypersurfaces in Affine Space 118
8.2.1 Invariants of isomorphic varieties 122
8.2.2 Inequivalent isomorphic varieties 124
8.3 The Embedding Conjecture for Free Associative Algebras 127

9 Coordinate Polynomials **129**
9.1 Coordinates of Two-Variable Polynomial Algebras 130
9.1.1 Proofs of main results 132
9.1.2 Algorithm for detecting coordinate polynomials . 136
9.1.3 Relation to the Jacobian Conjecture 137
9.2 Coordinates in Free Associative Algebra of Rank Two . . 138
9.2.1 Fox derivatives in a free associative algebra . . . 141
9.2.2 Proofs and algorithms 142
9.3 Density of Coordinates in Polynomial Algebras 144
9.4 Coordinates in $K[z][x, y]$ 147
9.4.1 Preliminaries 148

9.4.2 Characterization of tame and wild coordinates in $K[z][x,y]$ 151
9.4.3 New class of wild automorphisms 158

10 Test Polynomials **169**
10.1 Test Polynomials in Polynomial Algebras 171
10.2 Test Elements in Free Associative Algebras 174
10.3 Open Problems 180

III Free Nielsen–Schreier Algebras **183**

Introduction **185**

11 Schreier Varieties of Algebras **190**
11.1 Main Types of Nielsen–Schreier Algebras 191
11.2 Schreier Techniques 196
11.3 Free Differential Calculus 201
11.3.1 Free differential calculus and Schreier varieties . . 201
11.3.2 Ranks of subalgebras 207
11.4 Stable Equivalence 208
11.5 The Rank of an Endomorphism 210

12 Rank Theorems and Primitive Elements **213**
12.1 Basic Properties of Partial Derivatives 214
12.2 Homogeneous Admissible Elements 217
12.3 Elimination of Variables 219
12.4 Rank Theorems 225
12.5 Primitive Elements 229
12.5.1 Primitive elements in free nonassociative algebras 230
12.5.2 Primitive elements in free Lie superalgebras . . . 230
12.5.3 The Freiheitssatz and primitive elements 235
12.6 Primitive Elements and Endomorphisms 237
12.7 Inverse Images of Primitive Elements 241

13 Generalized Primitive Elements **244**
13.1 Test Elements 247
13.2 Retracts 252
13.3 Endomorphisms and Automorphic Orbits 254
13.4 Almost Primitive and Test Elements 256
13.5 Δ-Primitive Elements of Free Lie Algebras 262
13.6 Generic Elements of Free Lie Algebras 264

14 Free Leibniz Algebras **270**
14.1 Basic Notions 271
14.2 Differential Separability of Subalgebras 273

14.3 Residual Finiteness of Free Leibniz Algebras 275
14.4 Automorphisms of Free Leibniz Algebras 279
14.4.1 Simple automorphisms 279
14.4.2 Recognizing tame automorphisms 281

References **283**

Notation Index **306**

Author Index **308**

Subject Index **313**

Introduction

The main purpose of this book is to show how ideas from combinatorial group theory have spread to two other areas of mathematics: the theory of Lie algebras and affine algebraic geometry. Some of these ideas, in turn, came to combinatorial group theory from low-dimensional topology in the beginning of the 20th century through the work of several prominent topologists, such as M. Dehn, H. Tietze, J. Nielsen, H. Reidemeister, J. H. C. Whitehead, to name just a few. Very soon, combinatorial group theory became an independent area of mathematics with its own powerful techniques. New, purely combinatorial methods were created by O. Schreier, R. Fox, W. Magnus, A. G. Kurosh, R. C. Lyndon, and many others.

Then, in the 1950s, mostly through the work of A. I. Shirshov, several ideas from combinatorial group theory (most notably, Nielsen's and Schreier's techniques) have been adopted in the theory of Lie algebras; thus the combinatorial theory of Lie algebras was shaped, although the origins of the theory can be found in the papers (published in the 1930s) by P. Hall, W. Magnus, and E. Witt on the structure of free and nilpotent groups.

In the 1960s, combinatorial methods came to commutative algebra when B. Buchberger introduced what is now known as Gröbner bases. It is not very likely that Buchberger was directly influenced by ideas from combinatorial group theory, but his famous algorithm bears a resemblance to Nielsen's method, although in a more sophisticated form.

This book is in three fairly independent parts. In Part I, we first give a very brief exposition of several classical techniques in combinatorial group

theory, namely methods of Nielsen, Whitehead, and Tietze. We do not go into details because there are two very well-established monographs where a complete exposition of these techniques is given. For an exposition of Nielsen's method, we recommend [231], whereas [227] has, in our opinion, a better exposition of Whitehead's and Tietze's methods. Then we go on to very recent ideas and results. We focus here on the theory of free groups and their automorphisms since we believe that it is in the heart of combinatorial group theory. This does not mean, of course, that other areas, for instance the theory of braid groups or hyperbolic groups, are less significant.

We would also like to say up front that we only consider here purely combinatorial ideas and results; in particular, we leave out important interactions of group theory with topology and geometry. It should be pointed out that topological methods were recently used with great success in solving several difficult problems about free groups and their automorphisms. We only mention here seminal papers of J. R. Stallings [373] and M. Bestvina and M. Handel [51], but, in fact, many other people, notably G. Levitt, M. Lustig, M. Feighn, Z. Sela, E. Turner, J. McCool, W. Dicks, E. Ventura, K. Vogtmann, and S. Krstic, have contributed greatly to this area by employing topological techniques.

Part II contains the main focus of this book. Here, we show how the aforementioned techniques of combinatorial group theory have found their way into affine algebraic geometry, a fascinating area of mathematics that studies polynomials and polynomial mappings. An interesting thing about this area is that most of the research here is focused on five or six outstanding problems. The statements of those problems are rather elementary and can be understood by an average high school student. However, the problems have so far eluded all attempts at a complete solution, even though some of them have been settled in low dimensions. The relevant bibliography is really vast; however, most people who work(ed) in this area use(d) geometric methods. Notable exceptions are H. Bass, P. M. Cohn, W. Dicks, A. van den Essen, L. Makar-Limanov, J. McKay, S. S. Wang, and D. Wright.

The first major result about polynomial automorphisms that bears resemblance to the corresponding result in combinatorial group theory was the Jung–van der Kulk theorem [194] describing generators of the group of automorphisms of a polynomial algebra in two variables over a field. Then, more than 40 years later, the parallelism between the two areas came into play again, starting with the paper [124] and gradually attracting the attention of other people, including the authors of this book, V. Drensky, A. van den Essen, Z. Jelonek, W. Neumann, P. Wightwick, and others. One of the most significant results so far obtained by employing ideas from combinatorial group theory (in this case, Whitehead's idea of "peak reduction") is a recent solution of the automorphic equivalence problem for plane curves by Wightwick [401]. We believe that other ideas from combinatorial group theory also have a great potential in affine algebraic geometry, which was one of the main reasons for us to write this book.

It is remarkable that around the same time, in the mid-1990s, ideas from algebraic geometry found their way into combinatorial group theory. Perhaps an earlier paper of Lyndon [226] had a glimpse of such interaction, but it became really convincing through the work of G. Baumslag, A. G. Myasnikov, V. Remeslennikov, O. Kharlampovich [41, 176, 177, 285], and, essentially independently, B. I. Plotkin [308]. Thus, we have now a "two-way traffic" of ideas that allows algebraic geometry to shed light on group theory and vice versa!

In Part III, we show how ideas from combinatorial group theory contributed to the theory of free algebras. The focus here is on *Schreier varieties* of algebras (a variety of algebras is said to be Schreier if any subalgebra of a free algebra of this variety is free in the same variety of algebras). This includes varieties of Lie (super)algebras, of *all* algebras, and some others. Free algebras in these varieties admit an adoption of Nielsen's and Schreier's methods, which leads to a substantial parallelism between ideas and results in the two areas. We start Part III with basic properties of these algebras, Schreier's technique, free differential calculus, and differential separability of subalgebras. Then we consider automorphic orbits, combinatorial properties of (generalized) primitive elements, and fixed points of endomorphisms. Then we consider the variety of Leibniz algebras. Although it is not a Schreier variety, many of its combinatorial properties are similar to those of Schreier varieties.

We conclude the Introduction by comparing the present book to previously published ones on similar subject(s). There is an excellent monograph by A. van den Essen [122] that has some overlap with Part II of our book. We were trying to avoid too much overlap by focusing our attention here specifically on interactions between combinatorial group theory and affine algebraic geometry and not trying to survey *all* recent work in the latter area. We just give a very brief survey, in the beginning of each chapter, of the work related to a particular problem. Then, our Part III has some overlap with the monograph [275]; however, since [275] was published, there has been a lot of new work done in combinatorial theory of free algebras, so we emphasize this new work here.

Part I

Groups

Introduction to Part I

In this part, we first give a brief exposition of several classical techniques in combinatorial group theory, namely methods of Nielsen, Schreier, Whitehead, and Tietze (Chapter 1). We will need this in the subsequent parts of the book to show how these basic ideas of combinatorial group theory have penetrated affine algebraic geometry and the theory of Lie algebras. Also in Chapter 1, we give a brief exposition of Fox differential calculus; this technique, although not very popular among group theorists these days, sometimes provides new insights and suggests new directions of research. Also, it plays a rather important role in combinatorial theory of Lie algebras, where we do not have the facility of using powerful topological or geometrical methods.

Then we go on to recent ideas and results in the theory of free groups and their automorphisms. We leave out here important interactions of group theory with topology and geometry and focus on purely combinatorial methods having in mind, again, their future use in other parts of the book.

Chapter 2 is about *test elements*. The idea here is to distinguish, for example, automorphisms among arbitrary endomorphisms by means of their action on a single element, a test element. The first result of this particular type was that of Nielsen [293], who proved that if an endomorphism of the free group of rank 2 fixes the commutator of a pair of generators, then it is an automorphism. Similar results for other particular elements of a free group were later obtained by Zieschang [417, 418], Rosenberger [318], Dold [100], Rips [314], Durnev [115], and others. Shpilrain [352, 355] generalized most of these results and put them in perspective. Turner [383] characterized test elements of a free group as elements that do not belong to any

proper retract. Based on this characterization, Comerford [82] suggested an algorithm for recognizing test elements of a free group. The idea behind the definition of a test element has numerous ramifications; for example, one can consider properties (other than being an automorphism) of an endomorphism that can be recovered from its action on a single element. Also, one can consider *test sets* rather than just test elements. We discuss these and other ramifications in Chapter 2.

In Chapter 3, we consider various generalizations of primitive elements: *generic elements* in the sense of Stallings [375], *almost primitive elements* in the sense of Rosenberger [318], and Δ-*primitive elements* in the sense of Shpilrain [356]. It turns out that all these generalizations are related, but relations between them are rather nontrivial, which opens several interesting research avenues.

In the concluding chapter, Chapter 4, we deal with *automorphic orbits* in a free group F_n of finite rank; these are sets of the form $\{v \in F_n,\ v = \varphi(u)$ for some $\varphi \in \mathrm{Aut}(F_n)$ and a fixed $u \in F_n\}$. One special and very interesting automorphic orbit is the set of all *primitive elements* (these are automorphic images of a free generator of F_n). In particular, the following problem, along with its generalizations [352], has been a source of inspiration for several people: if an endomorphism φ of a free group F_n takes every primitive element to another primitive, is φ an automorphism? Recently, D. Lee [205] has settled this problem in the affirmative for every n. Other interesting problems arise from considering "abridged" orbits $\{v \in F_n;\ |v| = |u|,\ \varphi(v) = u$ for some $\varphi \in \mathrm{Aut}(F_n)\}$. For instance, the problem of counting primitive elements of a given length (see Problem (F17) in [42]) has received considerable attention lately.

1

Classical Techniques of Combinatorial Group Theory

In this chapter, we give a brief exposition of several classical techniques in combinatorial group theory, namely methods of Nielsen, Schreier, Whitehead, and Tietze and the free differential calculus due to Fox. We do not go into details here because there are two very well-established monographs where a complete exposition of these techniques is given. For an exposition of Nielsen's and Schreier's methods, we recommend [231], whereas [227] has, in our opinion, a better exposition of Whitehead's and Tietze's methods.

We emphasize the aspects of classical techniques of combinatorial group theory here that can be carried on to other areas of mathematics considered in this book, namely to affine algebraic geometry and the theory of free algebras.

1.1 Nielsen's Method

Let $F = F_n$ be the free group of a finite rank $n \geq 2$ with a set $X = \{x_1, \ldots, x_n\}$ of free generators. Let $Y = \{y_1, \ldots, y_m\}$ be an arbitrary finite set of elements of the group F. Consider the following elementary transformations that can be applied to Y:

(N1) y_i is replaced by $y_i y_j$ or by $y_j y_i$ for some $j \neq i$;

(N2) y_i is replaced by y_i^{-1};

(N3) y_i is replaced by some y_j, and at the same time y_j is replaced by y_i;

(N4) delete some y_i if $y_i = 1$.

It is understood that y_j does not change if $j \neq i$.

Every finite set of reduced words of F_n can be carried by a finite sequence of Nielsen transformations to a *Nielsen-reduced* set $U = \{u_1, \dots, u_k\}$; i.e., a set such that for any triple v_1, v_2, v_3 of the form $u_i^{\pm 1}$, the following three conditions hold:

(i) $v_1 \neq 1$;

(ii) $v_1 v_2 \neq 1$ implies $|v_1 v_2| \geq |v_1|, |v_2|$;

(iii) $v_1 v_2 \neq 1$ and $v_2 v_3 \neq 1$ implies $|v_1 v_2 v_3| > |v_1| - |v_2| + |v_3|$.

It is easy to see that if $U = (u_1, u_2, \dots u_k)$ is Nielsen-reduced, then the subgroup of F_n generated by U is free with a basis U.

One might notice that some of the transformations (N1)–(N4) are redundant; i.e., they are compositions of other ones. The reason behind that we will explain below.

We say that two sets Y and $\tilde{Y}$ are Nielsen equivalent if one of them can be obtained from another by applying a sequence of transformations (N1)–(N3). It was proved by Nielsen that two sets Y and $\tilde{Y}$ generate the same subgroup of the group F if and only if they are Nielsen equivalent. This result is now one of the central points in combinatorial group theory.

Note, however, that this result alone does not give an *algorithm* for deciding whether or not Y and $\tilde{Y}$ generate the same subgroup of F. To obtain an algorithm, we need to somehow define the *complexity* of a given set of elements and then show that a sequence of Nielsen transformations (N1)–(N3) can be arranged so that this complexity decreases (or, at least, does not increase) *at every step* (this is where we may need "redundant" elementary transformations!).

This was also done by Nielsen; the complexity of a given set $Y = \{y_1, \dots, y_m\}$ is just the sum of the lengths of the words $y_1, \dots, y_m$. Now the algorithm is as follows. Reduce both sets Y and $\tilde{Y}$ to Nielsen-reduced sets. This procedure is finite because the sum of the lengths of the words decreases at every step. Then solve the membership problem for every element of Y in the subgroup generated by $\tilde{Y}$ and vice versa.

Nielsen's method therefore yields (in particular) an algorithm for deciding whether or not a given endomorphism of a free group of finite rank is an automorphism.

Another classical method that we sketch in this section is that of Schreier. We are going to give a brief exposition of this method here in a special case of a free group; however, it is valid for arbitrary groups as well. We are going to use the same notation that we used before.

Let H be a subgroup of F. A *right coset representative function* for F (on the generators x_i) modulo H is a mapping of words in x_i, $w(x_1, x_2, \dots) \to \overline{w}(x_1, x_2, \dots)$, where the $\overline{w}(x_1, x_2, \dots)$ form a right coset representative system for F modulo H, which contains the empty word, and where

$\overline{w}(x_1, x_2, \dots)$ is the representative of the coset of $w(x_1, x_2, \dots)$. Then we have:

Theorem 1.1.1. *If $w \to \overline{w}$ is a right coset function for F modulo H, then H is generated by the words*

$$ux_i \cdot \overline{ux_i}^{-1},$$

where u is an arbitrary representative and x_i is a generator of F.

This already implies, for instance, that if F is finitely generated and H is a subgroup of finite index, then H is finitely generated.

Furthermore, a *Schreier right coset function* is one for which any initial segment of a representative is again a representative. The system of representatives is then called a *Schreier system.* It can be shown that there is always some Schreier system of representatives for F modulo H. Also, there is a *minimal Schreier system*; i.e., a Schreier system in which each representative has a length not exceeding the length of any word it represents. Not every Schreier system is minimal.

Example 1.1.2. Let F be the free group on a and b, and let H be the normal subgroup of F generated by a^2, b^2, and $aba^{-1}b^{-1}$. Then F/H has four cosets. The representative system $\{1, a, b, ab\}$ is Schreier, as is the representative system $\{1, a, b, ab^{-1}\}$. The representative system $\{1, a, b, a^{-1}b^{-1}\}$ is not Schreier; for, the initial segment a^{-1} of $a^{-1}b^{-1}$ is not a representative.

Using a *Reidemeister–Schreier rewriting process*, one can obtain a presentation (by generators and relators) for H. This implies, among other things, the following important result which has inspired a lot of research in other algebraic systems; some of this research is described in Part III of this book.

Theorem 1.1.3 (Nielsen–Schreier). *Every nontrivial subgroup H of a free group F is free.*

One can effectively obtain a set of free generating elements for H; namely, those $ux_i \cdot \overline{ux_i}^{-1}$ such that ux_i is not freely equal to a representative. Schreier obtained this set of free generators for H in 1927. In 1921, Nielsen, using quite a different method, had constructed a set of free generators for H if F was finitely generated. The generators of Nielsen are precisely those Schreier generators obtained when a minimal Schreier system is used.

We refer to [231, Chapter 3] for more details.

1.2 Whitehead's Method

A more difficult problem is, given a pair of elements of a free group F, to find out if one of them can be taken to the other by an automorphism of F. We call this problem *the automorphic conjugacy problem.* It was addressed by

Whitehead, who came up with another kind of elementary transformation in a free group. Let $X = \{x_1, x_2, \dots\}$ be a (finite) set of generators of the group F, and let $X^{-1} = \{x_1^{-1}, x_2^{-1}, \dots\}$

(W1) permutations on the set $X^{\pm 1} = X \cup X^{-1}$.

(W2) a transformation ω of the second type is defined by a set $S \subset X^{\pm 1}$ and a letter $a \in X^{\pm 1}$ with $a \in S$ and $a^{-1} \notin S$ in such a way that if $x \in X^{\pm 1}$, then

- **(a)** $\omega(x) = x$ provided $x = a^{\pm 1}$;
- **(b)** $\omega(x) = xa$ provided $x \neq a$, $x \in S$ and $x^{-1} \notin S$;
- **(c)** $\omega(x) = a^{-1}xa$ provided both $x, x^{-1} \in S$;
- **(d)** $\omega(x) = x$ provided both $x, x^{-1} \notin S$.

One might notice some similarity between Nielsen and Whitehead transformations. However, they differ in one essential detail: Nielsen transformations are applied to arbitrary sets of elements, whereas Whitehead transformations are applied to a *fixed basis* of the group F.

Using (informally) matrix language, we can say that Nielsen transformations correspond to elementary row transformations of a matrix (this correspondence can actually be made quite formal — see [353]), whereas Whitehead transformations correspond to conjugations (via changing the basis). This latter type of matrix transformation is known to be more complex, and the corresponding structural results are deeper.

There is pretty much the same relation between Nielsen and Whitehead transformations in a free group.

Note also that the Whitehead transformation (W2) is rather complex and it does not really look so "elementary". This is, again, in order to be able to arrange a sequence of elementary transformations so that the complexity of a given element (in this case, just the lexicographic length of a cyclically reduced word) would decrease (or, at least, not increase) *at every step.* To prove that this is possible, Whitehead has introduced a remarkable method called "peak reduction". This means that if in a sequence of elementary transformations the complexity goes up (or remains unchanged) before eventually going down, then there must be a pair of *subsequent* elementary transformations in the sequence (a "peak") such that one of them increases the complexity (or leaves it unchanged) and then the other one decreases it. Then one tries to prove that such a peak can always be reduced; i.e., replaced by (perhaps a sequense of) elementary transformations such that the complexity decreases at every step in the sequense.

This arrangement still leaves us with a difficult problem — to find out if one of two elements *of the same complexity* (meaning of the same length) can be taken to the other by an automorphism of F. This was always considered the most time-consuming part of Whitehead's algorithm, although

recent results in [286] make it appear likely that this part of the algorithm is fast, too.

In one special case, the second part of the algorithm is just not needed, namely where one of the elements is *primitive*; i.e., it is an automorphic image of x_1. If we have managed to reduce an element of a free group (by Whitehead transformations) to an element of length 1, we immediately conclude that it is primitive; no further analysis is needed.

1.3 Tietze's Method

Attempting to solve one of the major problems of combinatorial group theory, the isomorphism problem, Tietze introduced isomorphism-preserving elementary transformations that can be applied to groups presented by generators and relators.

Let

$$G = \langle x_1, x_2, \ldots \mid R_1, R_2, \ldots \rangle$$

be a presentation of a group $G = F/R$, where F is the ambient free group generated by $x_1, x_2, \ldots$, and R is the normal closure of $R_1, R_2, \ldots$; i.e., the smallest normal subgroup of F containing $R_1, R_2, \ldots$. Our treatment here is a little different from standard in that we apply elementary transformations to the whole normal subgroup R and not to a particular set $R_1, R_2, \ldots$ of relators. In other words, even though it looks like we specify $R_1, R_2, \ldots$ as defining relators, we do not consider them a preferred set of elements whose normal closure is R; we do this just for notational convenience.

The elementary transformations are of the following three types.

(T1) *Introducing a new generator*: Replace $\langle x_1, x_2, \ldots \mid R_1, R_2, \ldots \rangle$ by $\langle y, x_1, x_2, \ldots \mid yS^{-1}, R_1, R_2, \ldots \rangle$, where $S = S(x_1, x_2, \ldots)$ is an arbitrary element in the generators $x_1, x_2, \ldots$.

(T2) *Canceling a generator* (this is the converse of (T1)): If we have a presentation of the form $\langle y, x_1, x_2, \ldots \mid Q, R_1, R_2, \ldots \rangle$, where Q is of the form yS^{-1}, and $S, R_1, R_2, \ldots$ are in the group generated by $x_1, x_2, \ldots$, replace this presentation by $\langle x_1, x_2, \ldots \mid R_1, R_2, \ldots \rangle$.

(T3) *Renaming the generators*: Rename generators $(x_1, x_2, \ldots)$ to $(x_{i_1}, x_{i_2}, \ldots)$, where $i_1, i_2, \ldots$ are arbitrary distinct indices.

Then we have the following useful result due to Tietze (see, e.g., [227]):

Theorem 1.3.1. *Two groups* $\langle x_1, x_2, \ldots \mid R_1, R_2, \ldots \rangle$ *and* $\langle x_1, x_2, \ldots \mid S_1, S_2, \ldots \rangle$ *are isomorphic if and only if one can get from one of the presentations to the other by a sequence of transformations* (T1)–(T3).

For most practical purposes, groups under consideration are finitely presented, in which case there exists a finite sequence of transformations

(T1)–(T3) taking one of the presentations to the other. Still, Theorem 1.3.1 does not give any constructive procedure for deciding in a finite number of steps whether one finite presentation can be obtained from another by Tietze transformations because, for example, there is no indication of how to select the element S in a transformation (T1). Thus Theorem 1.3.1 does not yield a solution to the isomorphism problem.

However, it has been used in many situations to derive various invariants of isomorphic groups, most notably Alexander polynomials that turned out to be quite useful in knot theory (see, e.g., [85]).

Also, Tietze's method gives an easy, practical way of constructing "exotic" examples of isomorphic groups that helped to refute several conjectures in combinatorial group theory (see, e.g., our Section 1.4.1).

1.4 Free Differential Calculus

Let $\mathbb{Z}F$ be the integral group ring of a free group F and Δ its augmentation ideal; that is, the kernel of the natural homomorphism $\varepsilon\colon \mathbb{Z}F \to \mathbb{Z}$. More generally, when $R \leq F$ is a normal subgroup of F, we denote by Δ_R the ideal of $\mathbb{Z}F$ generated by all elements of the form $(r-1)$, $r \in R$. It is the kernel of the natural homomorphism $\varepsilon_R\colon \mathbb{Z}F \to \mathbb{Z}(F/R)$.

The ideal Δ is a free left $\mathbb{Z}F$-module with a free basis $\{(x_i - 1)\}$, $1 \leq i \leq n$, and left Fox derivations d_i are projections to the corresponding free cyclic direct summands. Thus any element $u \in \Delta$ can be uniquely written in the form $u = \sum_{i=1}^{n} d_i(u)(x_i - 1)$.

Since the ideal Δ is a free right $\mathbb{Z}F$-module as well, one can define right Fox derivatives $d_i'(u)$ accordingly so that $u = \sum_{i=1}^{n} (x_i - 1)d_i'(u)$.

One can extend these derivations linearly to the whole $\mathbb{Z}F$ by setting $d_i'(1) = d_i(1) = 0$.

Below we list several lemmas that we are going to need in subsequent chapters of the book. Most of the lemmas are standard, so we give them without proofs; an interested reader can find the proofs either in the original paper by Fox [134] or in the monograph by N. Gupta [146].

Lemma 1.4.1. *Let J be an arbitrary left (right) ideal of $\mathbb{Z}F$, and let $u \in \Delta$. Then $u \in \Delta J$ ($u \in J\Delta$) if and only if $d_i'(u) \in J$ ($d_i(u) \in J$) for each i, $1 \leq i \leq n$.*

Let $\gamma_k(R)$ denote the kth term of the lower central series of R.

Lemma 1.4.2. *Let R be a normal subgroup of F, and let $y \in F$. Then the following conditions are equivalent:*

(i) $y \in \gamma_{m+1}(R)$, $m \geq 1$,

(ii) $y - 1 \in \Delta_R \Delta^m$,

(iii) $y - 1 \in \Delta^m \Delta_R$.

This can be generalized to arbitrary subgroups R not necessarily normal. For an arbitrary R, we let Δ_R denote the *left* ideal of $\mathbb{Z}F$ generated by all elements of the form $(r-1)$, $r \in R$. Then we have:

Lemma 1.4.3. *Let R be a subgroup of F, and let $y \in F$. Then the following conditions are equivalent:*

(i) $y \in \gamma_{m+1}(R)$, $m \geq 1$,

(ii) $y - 1 \in \Delta^m \Delta_R$.

Before we formulate the next lemma, we have to introduce some more notation. If R is a normal subgroup of F, then there is a familiar action via conjugation of the group ring $\mathbb{Z}(F/R)$ on the abelian group R/R' under which R/R' becomes the relation module for F/R. Accordingly, there is a map $(F/R, R/R') \to R/R'$ defined by $(fR, rR') \to (f^{-1}rf)R'$ and linearly extended to $(\mathbb{Z}(F/R), R/R') \to R/R'$. Where the meaning is clear from the context, we denote the elements of $\mathbb{Z}F$ and their natural images in $\mathbb{Z}(F/R)$ by the same letters without ambiguity. Thus, for any $v \equiv \sum_i n_i f_i \bmod \mathbb{Z}F(R-1)$, $n_i \in \mathbb{Z}$, $f_i \in F$, and $r \in R$, the result of the action of $\sum_i n_i f_i R \in \mathbb{Z}(F/R)$ on rR' is denoted by $r^v R'$.

Lemma 1.4.4. *Let $r \in R$ and $v \in \mathbb{Z}F/\Delta_R$. If $r^v \equiv 1 \pmod{R'}$, then $v^* \partial r/\partial x_i \equiv 0 \pmod{\Delta_R}$ for every i, where for $v = \sum_i n_i f_i$, $v^* = \sum_i n_i f_i^{-1}$.*

We also need the "chain rule" for Fox derivations:

Lemma 1.4.5. *Let φ be an endomorphism of F (it can be linearly extended to $\mathbb{Z}F$) defined by $\varphi(x_k) = y_k$, $1 \leq k \leq n$, and let $v = \varphi(u)$ for some $u, v \in \mathbb{Z}F$. Then*

$$d_j(v) = \sum_{k=1}^{n} \varphi(d_k(u)) \cdot d_j(y_k),$$

$$d'_j(v) = \sum_{k=1}^{n} d'_j(y_k) \cdot \varphi(d'_k(u)).$$

For an endomorphism $\varphi\colon x_i \to y_i$, $1 \leq i \leq n$, of the group F_n, let $J_\varphi = (d_j(y_i))_{1 \leq i,j \leq n}$, $J'_\varphi = (d'_i(y_j))_{1 \leq i,j \leq n}$ be the Jacobian matrices of φ. We are going to need the following ramifications of Lemma 1.4.5.

Lemma 1.4.6. *If $g, h \in F_n$ and $h = \varphi(g)$, then for the "Fox gradients", one has*

$$(d_1(h), \ldots, d_n(h)) = (\varphi(d_1(g)), \ldots, \varphi(d_n(g))) \cdot J_\varphi,$$
$$(d'_1(h), \ldots, d'_n(h))^t = J'_\varphi \cdot (\varphi(d'_1(g)), \ldots, \varphi(d'_n(g)))^t,$$

where ^{t} means transposition.

Lemma 1.4.7. *If φ, ψ are two endomorphisms of F_n, then for the Jacobian matrices one has*

$$J_{\varphi(\psi)} = J_{\varphi}^{\psi} \cdot J_{\psi},$$
$$J'_{\varphi(\psi)} = J'_{\varphi} \cdot (J'_{\psi})^{\varphi}.$$

Now we give a nice application of Lemma 1.4.7 due to Birman [54]; it is usually called the "inverse function theorem" for free groups. The proof that we give here is easier than the original one.

Theorem 1.4.8 ([54]). *Let φ be an endomorphism of the free group F_n given by $\varphi\colon x_i \to y_i$, $1 \le i \le n$. Then $y_1, \dots, y_n$ generate the group F_n if and only if the Jacobian matrix J_φ is (left) invertible.*

Proof. The "only if" part of this theorem follows immediately from Lemma 1.4.7.

For the "if" part, recall that

$$y_j - 1 = \sum_{i=1}^{n} d_i(y_j)(x_i - 1). \tag{1.1}$$

Now suppose that the Jacobian matrix J_φ is left invertible over $\mathbb{Z}F$. From (1.1), we get then (in matrix form):

$$J_Y^{-1}(Y - 1) = X - 1,$$

where $Y - 1$ is $\{y_1 - 1, \dots, y_n - 1\}$ written as a column, and $X - 1$ is $\{x_1 - 1, \dots, x_n - 1\}$ written as a column. That means, for some elements $u_{ij} \in \mathbb{Z}F_n$ we have:

$$x_j - 1 = \sum_{i=1}^{n} u_{ij}(y_i - 1).$$

In other words, every $x_j - 1$ belongs to the left ideal of $\mathbb{Z}F_n$ generated by $\{y_1 - 1, \dots, y_n - 1\}$. By Lemma 1.4.12 in the next section, this implies that every x_j belongs to the subgroup generated by $\{y_1, \dots, y_n\}$; i.e., Y is a generating set of F. ■

Remark 1.4.9. Since the augmentation ideal of any group ring $\mathbb{Z}_pF_n$, p a prime, is a free left and right module over this ring, it is possible to consider Fox calculus in the rings $\mathbb{Z}_pF_n$ as well, and all technical results hold also in that situation. In particular, Birman's theorem, Theorem 1.4.8, holds upon replacing the Jacobian matrix J_φ by its natural homomorphic image over $\mathbb{Z}_pF_n$ for any prime p.

Finally, we give, without proofs, two ramifications of Theorem 1.4.8. The first one, due to Umirbaev [389], is a direct generalization of Birman's result:

Theorem 1.4.10 ([389]). *Let $(y_1, \dots, y_k)$, $1 \le k \le n$, be a system of elements of the group F_n. This system is primitive if and only if the matrix $(d_j(y_i))$, $1 \le i \le k$, $1 \le j \le n$ is left invertible over $\mathbb{Z}F_n$.*

The following ramification is due to Shpilrain [353]:

Theorem 1.4.11 ([353]). *An endomorphism $\varphi\colon x_i \to y_i$, $1 \le i \le n$, of the group F_n is a monomorphism if and only if the rows of the matrix $J_\varphi = (d_j(y_i))_{1 \le i,j \le n}$ are left $\mathbb{Z}F_n$-independent.*

1.4.1 Two applications

In this section, we give two very elegant applications of free differential calculus. One of them was previously published, the other was not. Neither of the two results is new; in fact, both can be considered classical. However, the proofs given here supersede (by far) the original proofs in simplicity and elegance. Also, the ideas used in these proofs will have more serious applications in Parts II and III of this book.

For the first application, we need one simple well-known fact about arbitrary group rings (see, e.g., [300]).

Lemma 1.4.12. *Let G be an arbitrary group, K an arbitrary commutative ring with unity, and KG the corresponding group ring. Let $v_1, \dots, v_m$ and u be elements of G. Suppose $(u-1)$ belongs to the left (or right) ideal of KG generated by $(v_1 - 1), \dots, (v_m - 1)$. Then u belongs to the subgroup H of G generated by $v_1, \dots, v_m$.*

Proof. Let S be an arbitrary subgroup of G and $u \in KG$ an arbitrary element of the group ring, so that $u = \sum_{g_i \in G} c_i g_i$, where $c_i \in K$. We introduce a mapping π_S on KG (a "projection") such that $\pi_S(u) = \sum_{g_i \in S} c_i g_i$. Then it is easy to see that this mapping is K-linear and, whenever $w \in KS$, one has $\pi_S(uw) = \pi_S(u) \cdot w$, and $\pi_S(wu) = w \cdot \pi_S(u)$.

Now let $g \in G$, $g - 1 = \sum w_i \cdot (v_i - 1)$ for some $w_i \in KG$. Apply π_H to both sides:

$$\pi_H(g) - 1 = \sum \pi_H(w_i) \cdot (v_i - 1).$$

If $g \notin H$, then $\pi_H(g) = 0$, so that the augmentation of the left-hand side of this equality is -1, whereas the augmentation of the right-hand side is 0. This contradiction implies $g \in H$. ∎

We are now in a position to give the first elegant application of free differential calculus. Specifically, we give a simple proof of the "if" part of Nielsen's "commutator test" (in a stronger form). Our notation here is $[a, b] = aba^{-1}b^{-1}$.

Proposition 1.4.13. *Let y_1 and y_2 be some elements of the free group F_2 generated by x_1 and x_2, and let R be the subgroup of F_2 generated by y_1 and y_2. If the commutator $[x_1, x_2]$ belongs to $[R, R]$, then $R = F_2$.*

Proof. By Lemma 1.4.2, we have

$$[x_1, x_2] - 1 \in \Delta\Delta_R. \tag{1.2}$$

Apply derivations d_1' and d_2' to both sides of (1.2):

$$x_1^{-1}x_2^{-1}(x_2[x_1, x_2] - 1) \in \Delta_R, \tag{1.3}$$

$$x_2^{-1}(x_2x_1^{-1}x_2^{-1} - 1) \in \Delta_R. \tag{1.4}$$

Now (1.3) implies $x_2[x_1, x_2] \in R$, and (1.4) implies $x_2x_1^{-1}x_2^{-1} \in R$, so we just have to show that these two elements generate F_2. Let $g = x_2[x_1, x_2]$, $h = x_2x_1^{-1}x_2^{-1}$. Then $hgh^{-1} = x_2$, so $x_2 \in R$, and $x_1 = x_2^{-1}gh^{-1}$, so $x_1 \in R$, and $R = F_2$. ∎

Remark 1.4.14. We can further strengthen Proposition 1.4.13 by claiming only $[x_1, x_2] \in R^2$ instead of $[x_1, x_2] \in [R, R]$. Indeed, on replacing the integral group ring with the ring $\mathbb{Z}_2F$, our argument remains valid because in $\mathbb{Z}_2F$ one has $r - 1 \in \Delta\Delta_R$ whenever $r \in R^2$.

The second elegant application of free differential calculus concerns a conjecture of Magnus refuted by McCool and Pietrowski in [241]. The conjecture was: given two elements g, h of a free group F such that the one-relator groups $\langle F \mid g\rangle$ and $\langle F \mid h\rangle$ are isomorphic, one has g conjugate to h by an automorphism of F.

The counterexample constructed in [241] was very simple; it was based on applying a nontrivial Tietze transformation (see Section 1.3) to a given one-relator group. The hard part was to show that two elements were not conjugate by an automorphism. Of course, one can apply Whitehead's method (see Section 1.2), but since there are a lot of elementary Whitehead transformations, this is technically rather complicated.

We give here a simple method for detecting automorphically inequivalent elements that is based on counting the number of "zeros" of the Fox gradients of given elements. The same idea plays an important role in Chapter 8 of this book.

Proposition 1.4.15. *Let F be the free group generated by x, y, and z, and let $g = x^{-1}y^2x^2z^2$, $h = x^{-1}y^2xz^2y^2xz^2$. Then the one-relator groups $\langle F \mid g\rangle$ and $\langle F \mid h\rangle$ are isomorphic, but g is not conjugate to h by any automorphism of F.*

Proof. The following sequence of Tietze transformations establishes the isomorphism:

$$\begin{aligned}
&\langle x, y, z \mid x^{-1}y^2x^2z^2 = 1\rangle = \langle x, y, z \mid x = y^2x^2z^2\rangle \\
&\cong \langle x, y, z, u \mid u = x^2,\ x = y^2uz^2\rangle \cong \langle y, z, , u \mid u = (y^2uz^2)^2\rangle \\
&\cong \langle x, y, z \mid x = (y^2xz^2)^2\rangle = \langle x, y, z \mid x^{-1}y^2xz^2y^2xz^2 = 1\rangle.
\end{aligned}$$

Now compute the *abelianized* Fox gradients of g and h:

$$\text{grad}^a(g) = (-x^{-1} + x^{-1}y^2 + y^2,\ x^{-1}(1+y),\ x^{-1}y^2x^2(1+z)),$$

$$\text{grad}^a(h)$$

$$= (-x^{-1} + x^{-1}y^2 + y^4z^2,\ x^{-1}(1+y)(1 + xz^2y^2),\ y^2(1+z)(1 + xz^2y^2)).$$

If we now allow x and y to take values in the group $\mathbb{C}^*$, we see that $\text{grad}^a(g)$ has no zeros, whereas $\text{grad}^a(h)$ has infinitely many zeros.

If g was an automorphic image of h, then $\text{grad}^a(g)$ and $\text{grad}^a(h)$ would have the same number of zeros by Lemma 1.4.6. This contradiction completes the proof. ■

2

Test Elements

This chapter is about *test elements* of various groups. The idea here is to distinguish, for example, automorphisms among arbitrary endomorphisms by means of their action on a single element, a test element. More precisely:

Definition 2.0.1 ([352]). An element $g \in G$ is called a test element (for recognizing automorphisms) of a group G if, whenever $\varphi(g) = g$ for an endomorphism φ of G, it follows that φ is an automorphism.

The condition "$\varphi(g) = g$" in this definition can be obviously replaced by "$\varphi(g) = \alpha(g)$ for some $\alpha \in \mathrm{Aut}(G)$". Thus, the definition can be informally rephrased as "if an endomorphism φ acts like an automorphism on one particular element g, then φ is itself an automorphism".

In this chapter, we are going to describe test elements in various groups, but the focus is on free groups. The first result of this particular type was that of Nielsen [293], who proved that if an endomorphism of the free group of rank 2 fixes the commutator of a pair of generators, then it is an automorphism. Similar results for other particular elements of a free group were later obtained by Zieschang [417, 418], Rosenberger [318], Dold [100], Rips [314], Durnev [115], and others. Shpilrain [352, 355] generalized most of these results and put them in perspective. Turner [383] characterized test elements of a free group as elements that do not belong to any proper retract. Based on this characterization, Comerford [82] suggested an algorithm for recognizing test elements of a free group.

The idea behind the definition of a test element has numerous ramifications; for example, one can consider properties (other than being an automorphism) of an endomorphism that can be recovered from its action

on a single element. Also, one can consider *test sets* rather than just test elements.

The situation in arbitrary groups is more complex. Turner and his students have several results on test elements in hyperbolic groups [289], direct products of groups [290], and free products of finite cyclic groups [396]. We concentrate here, in Section 2.1, on two-generator groups, where there were numerous attempts to expand Nielsen's "commutator test" to one-relator groups by Hill and Pride [151], to free metabelian groups by Durnev [115], and to free solvable and other groups by Gupta and Shpilrain [147].

There is also a nice application of test elements to solving equations in free groups pointed out by Durnev in [116].

In Section 2.3 of this chapter, we describe another result related to the idea of test elements. D. Lee [204], based on ideas of S. Ivanov [153], confirmed the following conjecture of Shpilrain [42, Problem (F7)]: every endomorphism of a free group of finite rank is completely determined by its values on just two (explicitly given) elements unless the image of this endomorphism is cyclic. We therefore have a test set of two elements that allows one to distinguish any two endomorphisms of a free group that have noncyclic images.

2.1 Nielsen's Commutator Test

Nielsen [293] gave the following commutator test for an endomorphism of the free group $F = F_2 = \langle x, y \rangle$ to be an automorphism: an endomorphism $\varphi\colon F \to F$ is an automorphism if and only if the commutator $[\varphi(x), \varphi(y)]$ is conjugate in F to $[x, y]^{\pm 1}$. He obtained this test as a corollary to his well-known result that every IA-automorphism of F (i.e., one that fixes F modulo its commutator subgroup) is an inner automorphism. Bachmuth et al. [29] have proved that IA-automorphisms of most two-generator groups of the type F/R' are inner, and it becomes natural to ask if Nielsen's commutator test remains valid for those groups as well. Durnev [115] considered this question for the free metabelian group F/F'' and confirmed the validity of the commutator test in this case. Here we will show that Nielsen's test does *not* hold for a large class of F/R' groups and, as a corollary, deduce that it does not hold for any nonmetabelian solvable group of the form F/R''. On the other hand, we give a sufficient condition under which Nielsen's commutator test is valid for a given pair of generating elements of F modulo $[R', F]$.

The negative result for F/R' groups yields the following natural question (see [43, Problem (S9)]): Does the free solvable group of rank 2 and derived length $d > 2$ have any test elements? Roman'kov [317] has constructed test elements in the free solvable group of rank 2 and derived length 3. It is plausible that the same method can be used for constructing test elements

in the free solvable group of any bigger rank as well, but technically it is getting more complicated.

We also mention a related result of Timoshenko [382], who proved that a free metabelian group of rank > 2 does *not* have any test elements.

Now we get to the main results of this section.

Theorem 2.1.1 ([147]). *Let $R \leq F'$ be a nontrivial normal subgroup of F such that*

(i) *the center of $F/[R,F]$ is $R/[R,F]$ and*

(ii) *the group ring $\mathbb{Z}(F/R)$ is an Ore domain (i.e., $\mathbb{Z}(F/R)$ has no zero divisors and any two nonzero elements have a common nonzero multiple).*

Then there exist $u, v \in F$ such that $[u,v] \equiv [x,y] \pmod{R'}$, while the endomorphism $x \to u$, $y \to v$ of F does not induce an automorphism of F/R'.

We need one preliminary lemma.

Lemma 2.1.2. *The mapping $\tau\colon x \to xr$, $y \to ys$ with $r, s \in F'$ defines an automorphism of F if and only if $r = [x,f]$ and $s = [y,f]$ for some $f \in F$. Similarly, the mapping $\tau'\colon x \to rx$, $y \to sy$ with $r, s \in F'$ defines an automorphism of F if and only if $r = [f, x^{-1}]$ and $s = [f, y^{-1}]$ for some $f \in F$.*

Proof. Consider an automorphism τ of F of the form

$$\tau\colon x \to xr,\ y \to ys \quad \text{where} \quad r, s \in F'.$$

Then τ is an IA-automorphism and hence, by Nielsen's characterization, τ must be an inner automorphism $x \to x^f$, $y \to y^f$, induced by some $f \in F$. Comparing the two formulations of τ yields the result. ■

Proof of Theorem 2.1.1. Choose some $r \in R$, $r \notin R'$. Let $u \equiv r^a x \pmod{R'}$ and $v \equiv r^b y \pmod{R'}$ for some $a, b \in \mathbb{Z}F$ (to be specified later). Then, modulo R', we have

$$\begin{aligned}
[r^a x, r^b, y] &\equiv [r^a x, y][r^a x, r^b]^y \equiv [r^a, y]^x [x,y][x, r^b]^y \\
&\equiv [x,y][r^a, y]^{x[x,y]}[x, r^b]^y \equiv [x,y][r^a, y]^{y^{-1}xy}[x, r^b]^y \\
&\equiv [x,y][y^{-1}, r^a]^{xy}[r^b, x^{-1}]^{xy} \equiv [x,y] r^{(a(1-y^{-1})+b(x^{-1}-1))xy}.
\end{aligned}$$

Thus, the congruence $[r^a x, r^b y] \equiv [x,y] \pmod{R'}$ is equivalent to the congruence

$$r^{(a(1-y^{-1})+b(x^{-1}-1))} \equiv 1 \pmod{R'}.$$

Since $\mathbb{Z}(F/R)$ has no zero divisors, it follows by Lemma 1.4.4 that

$$a(y^{-1}-1) \equiv b(x^{-1}-1) \ \text{ modulo } \ \Delta_R, \tag{2.1}$$

where $a, b \in \Delta_F$ (since $R \leq F'$ implies that Δ_R lies in Δ_F^2). By condition (ii) of our theorem, there exist $a, b \notin \Delta_R$ satisfying the congruence (2.1). We choose one such pair of elements a and b satisfying (2.1) and consider elements u and v of F such that

$$u \equiv r^a x \quad \text{and} \quad v \equiv r^b y \pmod{R'}.$$

For this choice of u and v, it is easy to see that the congruence $[u, v] \equiv [x, y] \pmod{R'}$ holds. Suppose that the mapping $x \to u$, $y \to v$ induces an automorphism of the group F/R'. Then, this being an IA-automorphism of F/R', it must be inner by a result of Bachmuth et al. [29]. In that case, as in Lemma 2.1.2, we would have, for some $f \in F$,

$$r^a \equiv [f, x^{-1}] \pmod{R'} \quad \text{and} \quad r^b \equiv [f, y^{-1}] \pmod{R'}. \tag{2.2}$$

Since r^a, r^b are in $[R, F]$ $(a, b \in \Delta_F)$, it follows that $f[R, F]$ is in the center of $F/[R, F]$, which by hypothesis is $R/[R, F]$. Thus $f \in R \setminus R'$. Now, (2.2) yields, by commuting appropriately with y^{-1} and x^{-1}, the congruences

$$r^{a(y^{-1}-1)} \equiv [f, x^{-1}, y^{-1}] \quad \text{and} \quad r^{b(x^{-1}-1)} \equiv [f, y^{-1}, x^{-1}] \pmod{R'},$$

which upon using (2.1) yield the congruence

$$[f, x^{-1}, y^{-1}] \equiv [f, y^{-1}, x^{-1}] \pmod{R'},$$

or, equivalently, $[f, x^{-1}y^{-1}] \equiv [f, y^{-1}x^{-1}] \pmod{R'}$, since $f \in R$. Now, an application of this last congruence in the expansion of the equation $[f, x^{-1}y^{-1}] = [f, [x, y]y^{-1}x^{-1}]$ modulo R' gives $[f, [x, y]] \in R'$, which implies (using Lemma 1.4.4) that $[y, x] \in R$, implying that F/R is abelian, contrary to the choice of R. This completes the proof of the theorem. ■

The following corollary to Theorem 2.1.1 contrasts sharply with the cited result of Durnev [115].

Corollary 2.1.3. *Let N be a proper normal subgroup of F such that F/N is solvable. Then there are elements u, v in F such that $[u, v] \equiv [x, y] \pmod{N''}$ but the endomorphism $x \to u$, $y \to v$ of F does not induce an automorphism of F/N''.*

Proof. Since F/N' is a torsion-free solvable group (see [146, p. 23], it follows by a theorem of Kropholler et al. [187] that the group ring $\mathbb{Z}(F/N')$ has no zero divisors. Thus, with $R = N'$, F/R is solvable and $\mathbb{Z}(F/R)$ has no zero divisors. It follows by a result of Lewin [214] that $\mathbb{Z}(F/R)$ is an Ore domain. Since the center of $F/[R, F]$ $(= F/[N', F])$ is always $R/[R, F]$ (see [146, p. 117]), the hypothesis of Theorem 2.1.1 is satisfied by R and the corollary follows. ■

Corollary 2.1.4.

(a) *For each $k \geq 3$, there exists an endomorphism $\varphi_k \colon F \to F$ that does not induce an automorphism of the free solvable group $F/F^{(k)}$*

of derived length k, whereas (by Corollary 2.1.3) $[\varphi_k(x), \varphi_k(y)] \equiv [x, y] \bmod F^{(k)}$;

(b) *For each $c \geq 3$, there exists an endomorphism $\psi_c \colon F \to F$ that does not induce an automorphism of $F/[\gamma_c(F), \gamma_c(F)]$, whereas $[\psi_c(x), \psi_c(y)] \equiv [x, y] \bmod [\gamma_c(F), \gamma_c(F)]$ (by Theorem 2.1.1).*

While Nielsen's commutator test does not hold for most F/R' groups of rank 2, the groups of the form $F/[R', F]$ behave altogether differently. Here we prove the following result.

Theorem 2.1.5 ([147]). *Let R be a nontrivial normal subgroup of the free group $F = \langle x, y; \varnothing \rangle$. If $[u, v] \equiv [x, y]^{\pm g} \bmod [R', F]$ for some $g \in F$, then u and v generate F modulo $[R', F]$.*

Proof. We may clearly assume that $[u, v] \equiv [x, y] \bmod [R', F]$. Since $[R', F] - 1 \leq \Delta_F \Delta_R \Delta_F$ (see, for instance, [146, p. 113]), we have

$$[u, v] \equiv [x, y] \pmod{\Delta_F \Delta_R \Delta_F}. \tag{2.3}$$

Taking right Fox derivatives of both sides of (2.3) yields

$$\begin{aligned} &\partial' u/\partial' x(v - [u, v]) + \partial' v/\partial' x(1 - v^{-1}uv) \equiv (y - [x, y]) \bmod \Delta_R \Delta_F, \\ &\partial' u/\partial' y(v - [u, v]) + \partial' v/\partial' y(1 - v^{-1}uv) \equiv (1 - y^{-1}xy) \bmod \Delta_R \Delta_F. \end{aligned} \tag{2.4}$$

Now, taking the left Fox derivatives of both sides of the congruences in (2.4) yields four congruences modulo Δ_R given by the following matrix equation:

$$\begin{pmatrix} \partial' u/\partial' x & \partial' v/\partial' x \\ \partial' u/\partial' y & \partial' v/\partial' y \end{pmatrix} \begin{pmatrix} \partial(v - [u, v])/\partial x & \partial(v - [u, v])/\partial y \\ \partial(1 - v^{-1}uv)/\partial x & \partial(1 - v^{-1}uv)/\partial y \end{pmatrix} = \begin{pmatrix} x^{-1}y^{-1}(y - 1) & 1 - x^{-1}y^{-1}(x - 1) \\ -y^{-1} & y^{-1} - y^{-1}x \end{pmatrix}.$$

It is easily verified that the matrix on the right-hand side above is invertible over $\mathbb{Z}F$ and hence also over $\mathbb{Z}F \pmod{\Delta_R}$. Hence the Jacobian matrix on the left-hand side is also invertible over $\mathbb{Z}F \pmod{\Delta_R}$, which, by a result of Krasnikov [186] (see [146, p. 29]), implies that u and v generate F modulo R'. It follows that u and v also generate F modulo any normal subgroup V of R such that R/V is nilpotent. Thus u and v generate F modulo $[R', F]$, as was to be proved. ■

Although the elements u and v generate the group $F/[R', F]$ under the conditions of Theorem 2.1.5, we cannot, in general, conclude that the mapping induced by $x \to u$, $y \to v$ defines an automorphism of the group $F/[R', F]$ since, for instance, $F/[R', F]$ may be non-Hopfian. Since $[R', F]$ might not be fully invariant in F, this mapping may not even define an endomorphism of $F/[R', F]$. As a (partial) converse of Theorem 2.1.5, we can prove the following result.

Proposition 2.1.6. *Let R be a normal subgroup of the free group F such that $R \leq F'$ and the group ring $\mathbb{Z}(F/R)$ has no zero divisors. If the mapping $\tau\colon x \to u,\ y \to v$ induces an automorphism of the group $F/[R', F]$, then $[u, v] \equiv [x, y]^{\pm g} \bmod [R', F]$ for some $g \in F$.*

Proof. Let τ induce some automorphism ψ of the group F/R'. Then ψ is tame (Bachmuth et al. [29]) and hence a composition of inner automorphisms of F/R' together with the automorphisms of F/R' induced by the maps $x \to y,\ y \to x$ and $x \to xy,\ y \to y$. It suffices, therefore, to verify that the congruence $[\tau(x), \tau(y)] \equiv [x, y]^{\pm g} \bmod [R', F]$ holds for some g in F when τ is assumed to be an inner automorphism of $F/[R', F]$ or else defined by the maps $x \to y,\ y \to x$ and $x \to xy,\ y \to y$. These verifications are straightforward, and we omit the details. ■

2.2 Recognizing Test Elements

In this section, we give a remarkable characterization, due to Turner [383], of test elements in a free group of finite rank along with some other interesting auxiliary results. Then, based on Turner's characterization, we describe an algorithm, due to Comerford [82], for recognizing test elements.

We denote by $F_r = F(x_1, \ldots, x_r)$ the free group of rank $r \geq 2$ with basis $\{x_1, \ldots, x_r\}$ and by F a free group of unspecified rank.

Definition 2.2.1 ([352]). The *rank* of $w \in F$ is the smallest rank of a free factor of F containing w.

It is clear that if w is a test word, then w has maximal rank. The following example shows that the converse is not true in general.

Example 2.2.2. Let $\varphi\colon F_2 \to F_2$ be defined by

$$\varphi(x_1) = x_1^2 x_2 x_1^{-1} x_2^{-1}, \quad \varphi(x_2) = 1.$$

Then φ fixes $x_1^2 x_2 x_1^{-1} x_2^{-1}$, but $x_1^2 x_2 x_1^{-1} x_2^{-1}$ lies in no proper free factor (see, for example, [71, p. 139]).

What distinguishes $x_1^2 x_2 x_1^{-1} x_2^{-1}$ from, say, $x_1 x_2 x_1^{-1} x_2^{-1}$ is that the former lies in a proper retract (namely, the image of φ) while the latter does not. We recall the definition of a retract:

Definition 2.2.3. A *retract* R of a group G is a subgroup with the property that the identity map $i\colon R \to R$ extends to a homomorphism $\rho\colon G \to R$. Equivalently, a *retraction* $\rho\colon G \to G$ is a homomorphism such that $\rho^2 = \rho$ and a retract is the image of a retraction.

Free factors are retracts, but not all retracts of free groups are free factors. The next definition is important for what follows.

Definition 2.2.4 ([152]). If $\varphi\colon F \to F$ is an endomorphism of the free group F, then the *stable image* of φ is

$$\varphi^\infty(F) = \bigcap_{i=0}^{\infty} \varphi^i(F), \quad \text{and} \quad \varphi_\infty = \varphi \mid \varphi^\infty(F).$$

It is shown in [152] that φ_∞ is an automorphism and clearly $\varphi^\infty(F)$ contains $\mathrm{Fix}(\varphi)$, the set of words fixed by φ.

Theorem 2.2.5 ([383]). *If $\varphi\colon F \to F$ is an endomorphism of the finitely generated free group F, then $\varphi^\infty(F)$ is a retract of F; $\varphi^\infty(F)$ is a proper retract precisely when φ fails to be an automorphism. If φ is a monomorphism, then $\varphi^\infty(F)$ is a free factor.*

Proof. It follows from [231, Problem 33, p. 118] (see also [152]) that $\varphi^\infty(F)$ is a free factor of $\varphi^n(F)$ for almost all n. Choose a particular such n, let $\hat{F}$ be a complementary free factor, and consider

$$\varphi^n\colon F \to \varphi^n(F) = \varphi^\infty(F) * \hat{F}.$$

If φ is a monomorphism, then $\varphi^n\colon F \to \varphi^n(F)$ is an isomorphism, so letting $F' = (\varphi^n)^{-1}(\hat{F})$,

$$F = (\varphi^n)^{-1}(\varphi^\infty(F)) * (\varphi^n)^{-1}(\hat{F}) = \varphi^\infty(F) * F'.$$

More generally, let $\pi\colon \varphi^n(F) \to \varphi^\infty(F)$ be a projection on the first factor of the decomposition above. If ρ is the composition $\rho = (\varphi_\infty^{-1})^n \circ \pi \circ \varphi^n$,

$$F \xrightarrow{\varphi^n} \varphi^n(F) \xrightarrow{\pi} \varphi^\infty(F) \xrightarrow{(\varphi_\infty^{-1})^n} \varphi^\infty(F),$$

then ρ is a retraction. ■

Corollary 2.2.6. *The test words in F are the words not contained in proper retracts. The test words for monomorphisms in F_r are the words of rank r.*

Proof. We show that w is not a test word if and only if w is contained in a proper retract. It is clear that if w lies in a proper retract, then it is not a test word since it is fixed by the retraction that is not an automorphism. Conversely, suppose that $w \in F$ is not a test word and that φ is an endomorphism fixing w that is not an automorphism. Then, by Theorem 2.2.5, $\varphi^\infty(F)$ is a proper retract containing w.

If w is not a test word for monomorphisms and is fixed by the monomorphism μ that is not an automorphism, then $w \in \mu^\infty(F)$, which is a proper free factor; thus w has nonmaximal rank. ■

Example 2.2.7. The following are test elements in a free group F_n: $x_1^k \cdot \cdots \cdot x_n^k$, $k \geq 2$, $[x_1, \ldots, x_n]$, $[x_1, x_2] \ldots [x_{2m-1}, x_{2m}]$ if $n = 2m$.

In a special case $n = 2$, test elements can be described more explicitly. Let $\sigma_{x_i}(u)$ be the sum of the exponents to which x_i occurs in the word u.

Corollary 2.2.8. *A word $u \in F_2$, which is not a proper power, is a test word if and only if* $\mathrm{g.c.d.}(\sigma_{x_1}(u), \sigma_{x_2}(u)) > 1$. *In particular, every* $u \in [F_2, F_2]$ *is a test word.*

Proof. Suppose first that $\mathrm{g.c.d.}(\sigma_{x_1}(u), \sigma_{x_2}(u)) = 1$. Then, upon taking x_1 and x_2 to appropriate powers of x_1, we can take u to x_1 by an endomorphism. Then apply another endomorphism, taking x_1 to u and x_2 to 1. The composition of these two endomorphisms is a retraction that takes F_2 onto the subgroup generated by u. Thus, u belongs to a proper retract of F_2 and therefore is not a test word by Corollary 2.2.6.

If $\mathrm{g.c.d.}(\sigma_{x_1}(u), \sigma_{x_2}(u)) > 1$, then any automorphic image of u has the same property. Suppose, by way of contradiction, that u belongs to a proper retract of F_2. Since every proper retract of F_2 is cyclic and u is not a proper power, u must be a generator of a proper retract. Then, by [231, p. 140], upon applying an automorphism to u, we can take it to an element of the form $x_1 \cdot c$, where c belongs to the normal closure of x_2. In an element v of this form, one has $\sigma_{x_1}(v) = 1$, hence $\mathrm{g.c.d.}(\sigma_{x_1}(v), \sigma_{x_2}(v)) = 1$, a contradiction. Thus, u does not belong to any proper retract of F_2 and therefore is a test word by Corollary 2.2.6. ■

For free groups of higher rank, the situation is more complex, and an algorithm for recognizing test elements is more sophisticated. Before we describe this algorithm (due to Comerford [82]), we give an example (due to D. Voce) showing that Turner's characterization of test elements may not hold in nonfree groups. More precisely, test elements can never lie in proper retracts, but there might be elements that do not lie in any proper retract and yet are not test elements.

Example 2.2.9. In the group K presented by $\langle a, b \mid aba^{-1} = b^{-1} \rangle$, b lies in no proper retract, but the endomorphism φ defined by

$$\varphi(a) = a^3 b, \quad \varphi(b) = b$$

is not surjective. Furthermore, $\varphi^\infty(K) = \langle b \rangle$, showing that Theorem 2.2.5 does not generalize to K.

Now we get to Comerford's algorithm for recognizing test elements in a free group. Here we shall use the following terminology and notation. We let G and H be free groups freely generated by sets A and B, respectively; when we speak of lengths of elements of H and G, it will be with respect to these generating sets. If $\alpha\colon H \to G$ is a homomorphism, we say that $w \in G$ is a *Nielsen-reduced image* of $u \in H$ under α if $\alpha(u) = w$, $u = s_1 \dots s_k$ with $s_1, \dots, s_k \in B \cup B^{-1}$, $s_{i+1} \neq s_i^{-1}$ for $1 \leq i \leq k-1$ and, as reduced words on $A \cup A^{-1}$, $\alpha(s_1), \dots, \alpha(s_k)$ satisfy

$$\begin{aligned}
&\alpha(s_i) \neq 1 && \text{for } 1 \leq i \leq k, \\
&|\alpha(s_i s_{i+1})| \geq |\alpha(s_i)|, |\alpha(s_{i+1})| && \text{for } 1 \leq i \leq k-1, \quad \text{and} \\
&|\alpha(s_i s_{i+1} s_{i+2})| > |\alpha(s_i)| - |\alpha(s_{i+1})| + |\alpha(s_{i+2})| && \text{for } 1 \leq i \leq k-2.
\end{aligned}$$

In other words, no letter of u has an empty image under α, not more than half the image of a letter of u cancels with the image of an adjacent letter of u, and no interior letter of u has its image cancelled entirely by the images of the two adjacent letters.

Given a homomorphism $\alpha\colon H \to G$ with $\alpha(u) = w$, we want to produce an endomorphism τ of H and a homomorphism $\beta\colon H \to G$ such that w is a Nielsen-reduced image of $\tau(u)$ under β. We use a Nielsen reduction technique similar to that employed by Lyndon in [225]. Following Lyndon, we call an automorphism of H defined by $s \mapsto st^{-1}$ with $s, t \in B \cup B^{-1}$ and $t \neq s^{\pm 1}$ and $f\colon b \mapsto b$ for $b \in B$, $b \neq s^{\pm 1}$, an *elementary regular transformation*. This transformation is *attached* to a reduced $u \in H$ if st or $t^{-1}s^{-1}$ is a subword of u. We also include the identity map on H as an elementary regular transformation attached to every element of H. An endomorphism of H defined by $c \mapsto 1$ for some $c \in B$ and $b \mapsto b$ for $b \in B - \{c\}$ is called an *elementary singular transformation* and is *attached* to a reduced $u \in H$ if c or c^{-1} occurs in u. A *Nielsen transformation* is an endomorphism τ of H of the form $\tau = \tau_1 \dots \tau_k$, where each τ is an elementary regular or singular transformation; we call τ *regular* or *singular* if each factor τ_i is regular or each τ_i is singular. We say that τ is *attached* to $u \in H$ if τ_i is attached to $\tau_1 \dots \tau_{i-1}(u)$ for $1 \leq i \leq k$.

We also need the notion of the *star graph* (or *co-initial graph* or *Whitehead graph*) $\Sigma(u)$ of a reduced $u \in H$. The set of vertices of $\Sigma(u)$ is $B \cup B^{-1}$. For each subword st of u with $s, t \in B \cup B^{-1}$, $\Sigma(u)$ has a directed edge from s to t^{-1}; if p and q are the terminal and initial letters of u, $\Sigma(u)$ also has an edge from p to q^{-1} called the *external edge*. For a subset S of $B \cup B^{-1}$, the *subgraph of* $\Sigma(u)$ *spanned by* S is a graph with set S of vertices and with edges being those edges of $\Sigma(u)$ both of whose endpoints lie in S. We say that $u \in H$ is *connected* if the subgraph of $\Sigma(u)$ spanned by $\mathrm{gen}(u) \cup (\mathrm{gen}(u))^{-1}$ is connected, where $\mathrm{gen}(u) = \{b \in B\colon\ b \text{ or } b^{-1} \text{ occurs in } u\}$.

We shall also make use of Whitehead automorphisms of H. They are of two types. The first, called *level Whitehead automorphisms*, simply permute $B \cup B^{-1}$. The second type of Whitehead automorphism is denoted (S, s), where $S \subseteq B \cup B^{-1}$ with $s \in S$ and $s^{-1} \notin S$. The map (S, s) is defined by $t \mapsto ts$ if $t \in S$, $t^{-1} \notin S$, and $t \neq s$, by $t \mapsto s^{-1}ts$ if $t, t^{-1} \in S$, and by $b \mapsto b$ if $b \in B$, $b, b^{-1} \notin S$, or $b = s$ or s^{-1}. A Whitehead automorphism (S, s) is *attached* to a reduced word $u \in H$ if the subgraph of $\Sigma(u)$ spanned by S is connected. We observe the following:

Lemma 2.2.10. *Every Whitehead automorphism (S, s) attached to a reduced word $u \in H$ is a regular Nielsen transformation attached to u.*

Proof. We use induction on $|S|$, the number of elements of S. If $|S| = 1$, $S = \{s\}$ and (S, s) is the identity map. If $|S| \geq 2$, choose $t \in S$ such that $t \neq s$ but t and s are joined by an edge in $\Sigma(u)$. It is easy to see that $(S, s) = (\{t, s\}, s)(S - \{t\}, s)$ and that $(\{t, s\}, s)$ is an elementary regular

transformation attached to u. It remains to show that $(S-\{t\}, s)$ is attached to $\varrho(u)$, where $\varrho = (\{t, s\}, s)$.

If $S - \{t\} = \{s\}$, we are finished, so suppose that $p \in S - \{t\}$, $p \neq s$. Since (S, s) is attached to u, there is an edge-path $e_1 \dots e_k$ in $\Sigma(u)$ with e_i an edge from p_{i-1} to p_i, $p_i \in S$ for $0 \leq i \leq k$, $p_0 = p$, and $p_k = s$; among all such edge-paths, pick one with k minimal. If $p_i \neq t$ for $0 \leq i \leq k$, then $e_1 \dots e_k$ is an edge-path in $\Sigma(\varrho(u))$ witnessing that p and s are in the same component of the subgraph of $\Sigma(\varrho(u))$ spanned by $S - \{t\}$. If $p_i = t$ for some i, $0 \leq i \leq k$, our choice of edge-path shows that $p_{k-1} = t$ and $p_i \neq t$ for $0 \leq k - 1$. In $\Sigma(\varrho(u))$ there is an edge e'_{k-1} from p_{k-2} to s, and so $e_1 \dots e_{k-2} e'_{k-1}$ is an edge-path from p to s in the subgraph of $\Sigma(\varrho(u))$ spanned by $S - \{t\}$. It follows that the subgraph of $\Sigma(\varrho(u))$ spanned by $S - \{t\}$ is connected, and so $(S - \{t\}, s)$ is attached to $\varrho(u)$. ■

We are now ready to prove the following generalization of [225, Proposition 6].

Proposition 2.2.11. *If G and H are free groups freely generated by sets A and B, respectively, and if $u \in H$, $w \in G$, and $\alpha\colon H \to G$ is a homomorphism with $\alpha(u) = w$, then there is a Nielsen transformation τ of H attached to u and a homomorphism $\beta\colon H \to G$ such that $\tau(u)$ is connected, w is a Nielsen-reduced image of $\tau(u)$ under β, and $\beta(H) = \alpha(H)$.*

Proof. The proof here is, for the most part, a standard Nielsen reduction argument. We make use of a function K introduced in [225]; K is a map from G to the positive integers with the properties that $|u| \leq |v|$ implies $K(u) \leq K(v)$ and that $K(u) = K(v)$ if and only if $u = v$ or $u = v^{-1}$. We use induction, first on $|\operatorname{gen}(u)|$, the number of generators of H occurring in u, and second on $\sum_{b \in \operatorname{gen}(u)} K(\alpha(b))$. If u is not connected, there is some $s \in \operatorname{gen}(u)$ such that s and s^{-1} are in different components of $\Sigma(u)$. At least one of these components, say that of s, fails to contain the external edge. We let S be the set of vertices in the component of s in $\Sigma(u)$ and note that (S, s) is attached to u, that $|\operatorname{gen}((u)(S, s))| \leq |\operatorname{gen}(u)|$, and that $\alpha((H)(S, s)^{-1}) = \alpha(H)$. We replace u by $(u)(S, s)$ and α by $(S, s)^{-1}\alpha$ and appeal to the induction hypothesis.

Suppose now that u is connected and that $\alpha(c) = 1$ for some $c \in \operatorname{gen}(u)$. In this case, we use the Nielsen transformation τ defined by $\tau(c) = 1$ and $\tau(b) = b$ for $b \in B - \{c\}$. Now τ is attached to u and $|\operatorname{gen}(\tau(u))| \leq |\operatorname{gen}(u)|$, so we may replace u by $\tau(u)$ and again invoke the induction hypothesis.

Finally, suppose that u is connected and $\alpha(b) \neq 1$ for $b \in \operatorname{gen}(u)$ but that w is not a Nielsen-reduced image of u under α. Then either u has a subword st with $s, t \in B \cup B^{-1}$ and more than half of either $\alpha(s)$ or $\alpha(t)$ cancels in the product $\alpha(s)\alpha(t)$, or u has a subword rst with $r, s, t \in B \cup B^{-1}$ and $\alpha(s)$ cancels entirely in the product $\alpha(r)\alpha(s)\alpha(t)$. As in the proof of [225, Lemma 3], there is an elementary regular Nielsen transformation τ attached to u such that $|\operatorname{gen}(\tau(u))| \leq |\operatorname{gen}(u)|$ and

$\sum_{b\in\mathrm{gen}(\tau(u))} K((\tau^{-1}\alpha(b))) \leq \sum_{b\in\mathrm{gen}(u)} K(\alpha(b))$. Here we replace u by $\tau(u)$, α by $\tau^{-1}\alpha$ (notice that $\tau^{-1}\alpha(H) = \alpha(H)$), and use the induction hypothesis. ■

Theorem 2.2.12. *There is an algorithm to tell which elements of a free group G are test elements; that is, to decide for $w \in G$ whether or not every endomorphism α of G with $\alpha(w) = w$ is an automorphism of G.*

Proof. Let us fix a free generating set A for G. We may assume that A is finite, for otherwise no element of G is a test element. If $w \in G$ and α is an endomorphism of G with $\alpha(w) = w$, then by Proposition 2.2.11 there are endomorphisms τ and β of G such that w is a Nielsen-reduced image of $\tau(w)$ under β. We can effectively enumerate the pairs $(v_1, \beta_1), \ldots, (v_2, \beta_k)$ such that w is a Nielsen-reduced image of $v_i \in G$ under the endomorphism β_i of G, but β_i is not surjective. (If $|A| \geq 2$, there will be such pairs. For example, if $A = \{a_1, a_2, \ldots, a_n\}$, we have the pair (a_1, β) with $\beta(a_1) = w$ and $\beta(a_i) = 1$ for $2 \leq i \leq n$.) We next check to see if any of $v_1, \ldots, v_k$ are endomorphic images of w in G; this is decidable by Makanin's algorithm [232] to tell if equations have solutions in a free group. If one of $v_1, \ldots, v_k$ is an endomorphic image of w in G, then w is not a test element for G; otherwise, w is a test element for G. ■

2.3 Test Sets

One can consider test sets rather than just single test elements. This allows one to detect more subtle distinctions between different automorphisms of a free group. In particular, the following natural problem has attracted a lot of attention:

Problem 2.3.1 ([43]). Denote by $\mathrm{Epi}(n, k)$ the set of all homomorphisms from a free group F_n onto a free group F_k; $n, k \geq 2$. Are there two elements $g_1, g_2 \in F_n$ with the following property: whenever $\varphi(g_i) = \psi(g_i)$, $i = 1, 2$, for some homomorphisms $\varphi, \psi \in \mathrm{Epi}(n, k)$, then $\varphi = \psi$? (In other words, every homomorphism from $\mathrm{Epi}(n, k)$ is completely determined by its values on just two elements.)

Addressing this problem, S. Ivanov [153] proved that every *injective* homomorphism from $\mathrm{Epi}(n, k)$ is completely determined by its values on just two elements.

More recently, D. Lee [204], based on the ideas of [153], settled the problem completely. Below we sketch some ideas from Ivanov's paper [153] and refer the reader to [153] and [204] for full proofs.

Definition 2.3.2. A nontrivial element $w \in F_m$ is an M-test word for F_m if for every endomorphism φ and monomorphism ψ of F_m the equation $\varphi(w) = \psi(w)$ implies that φ is also a monomorphism.

Definition 2.3.3. A nontrivial word $w(x_1, \dots, x_n)$ is a C-test word in n letters for F_m if for any two n-tuples $(A_1, \dots, A_n)$, $(B_1, \dots, B_n)$ of elements of F_m the equality $w(A_1, \dots, A_n) = w(B_1, \dots, B_n) \neq 1$ implies the existence of an element $S \in F_m$ such that $B_i = SA_iS^{-1}$ for all $i = 1, 2, \dots, n$.

We can make several observations related to Definitions 2.3.2–2.3.3. First, any C-test word in n letters is both a test and M-test element for F_n. In this sense, Definition 2.3.3 is the most restrictive one. The commutator $[x_1, x_2]$ is an M-test word (for F_2) but not a C-test word in two letters. If a C-test word w in n letters is not a proper power, then the stabilizer of w in $\operatorname{Aut} F_n$ is $\langle \tau_w \rangle$.

The word $w = [x_1, x_2][x_3, x_4] \dots [x_{2m-1}, x_{2m}]$ with $m > 1$ is neither a C- nor M-test one. To see the latter, consider an even m and put $A_1 = x_1, \dots$, $A_m = x_m$, $A_{m+1} = x_{2m}x_m x_{2m}^{-1}$, $A_{m+2} = x_{2m}x_{m-1}x_{2m}^{-1}, \dots$, $A_{2m-1} = x_{2m}x_2x_{2m}^{-1}$, $A_{2m} = x_{2m}x_1x_{2m}^{-1}$. Then $\operatorname{rank}\langle A_1, \dots, A_{2m} \rangle = 2m$ but

$$[A_1, A_2][A_3, A_4] \dots [A_{2m-1}, A_{2m}] = [[x_1, x_2] \dots [x_{m-1}, x_m], x_{2m}].$$

Therefore, setting $\varphi(x_1) = [x_1, x_2] \dots [x_{m-1}, x_m]$, $\varphi(x_2) = x_{2m}$, $\varphi(x_3) = \dots = \varphi(x_{2m}) = 1$, we see that w fails to be an M-test word. Clearly, a similar argument can be used to consider the case of odd $m > 1$.

It is not clear whether or not there are M-test words in F_m, $m \geq 3$, among the words of the form $x_1^{k_1} \dots x_m^{k_m}$, and this might be a rather interesting and difficult problem. If $m = 2$, then any word $x_1^{k_1}x_2^{k_2}$, where k_1, k_2 are multiples of $k > 1$, is an M-test word. This follows from a result of Lyndon and Schützenberger [228] that elements of a solution of the equation $x^{l_1}y^{l_2}z^{l_3} = 1$ with $l_i > 1$ in F_m lie in a cyclic subgroup.

On the other hand, it is easy to see from considering values of a C-test word $w(x_1, \dots, x_n)$ on a cyclic subgroup of F_m that if $n > 1$ then $w \in F_n'$, where F_n' is the commutator subgroup of the free group F_n with basis $\{x_1, \dots, x_n\}$. This implies that there are no C-test words among the words $x_1^{k_1} \dots x_m^{k_m}$.

The words $[x_1, \dots, x_m]$ with $m > 2$ are neither M- nor C-test ones. To see this, put $A_1 = x_3x_1x_3^{-1}$, $A_2 = x_3x_2x_3^{-1}$, $A_3 = [x_1, x_2]$. Then $\operatorname{rank}\langle A_1, A_2, A_3 \rangle = 3$ and

$$[[A_1, A_2], A_3] = [x_3[x_1, x_3]x_3^{-1}, [x_1, x_2]] = [[x_3, [x_1, x_2]], [x_1, x_2]].$$

Hence, upon setting $\varphi(x_1) = x_3$, $\varphi(x_2) = \varphi(x_3) = [x_1, x_2]$, we see that $[[x_1, x_2], x_3]$ is not an M-test word, and now the claim becomes obvious.

Thus, Definitions 2.3.2–2.3.3 are rather restrictive, and the very existence of M-test words for F_m, $m > 2$, and, especially, C-test words in n letters for F_m with $m, n > 1$ is unclear. However, it turns out that C-test words do exist.

Theorem 2.3.4 ([153]). *For arbitrary $n \geq 2$, there exists a word $w_n(x_1, \ldots, x_n)$ that is a C-test word in n letters for any free group F_m of rank $m \geq 2$. In addition, $w_n(x_1, \ldots, x_n)$ is not a proper power.*

Corollary 2.3.5. *There is an element $u \in F_m$ such that if φ is an endomorphism, ψ is a monomorphism of F_m, and $\varphi(u) = \psi(u)$, then φ is also a monomorphism and, more specifically, $\varphi = \tau_u^k \psi$, where τ_u is the inner automorphism of F_m defined by means of u and k is an integer.*

Corollary 2.3.6. *There are two elements $u_1, u_2 \in F_m$ such that any monomorphism ψ of F_m is uniquely determined by $\psi(u_1), \psi(u_2)$.*

Corollaries 2.3.5 and 2.3.6 follow immediately from Theorem 2.3.4: It suffices to put $u = w_m(x_1, \ldots, x_m)$ in Corollary 2.3.5 and $u_1 = w_m(x_1, \ldots, x_m)$, $u_2 \notin \langle w_m(x_1, \ldots, x_m) \rangle$ in Corollary 2.3.6.

The construction of the C-test word $w_n(x_1, \ldots, x_n)$ is as follows: If $n = 2$, then

$$w_2(x_1, x_2) = [x_1^8, x_2^8]^{100} x_1 [x_1^8, x_2^8]^{200} x_1 [x_1^8, x_2^8]^{300} x_1^{-1} [x_1^8, x_2^8]^{400} \times x_1^{-1} [x_1^8, x_2^8]^{500} x_2 [x_1^8, x_2^8]^{600} x_2 [x_1^8, x_2^8]^{700} x_2^{-1} [x_1^8, x_2^8]^{800} x_2^{-1}.$$

For $n \geq 3$,

$$w_n(x_1, \ldots, x_n) = w_2(w_{n-1}(x_1, \ldots, x_{n-1}), w_{n-1}(x_2, \ldots, x_n)).$$

To conclude this section, we give a definition of the *test rank* of a finitely generated group G:

Definition 2.3.7. Let G be an n-generator group. Call a set of elements $\{g_1, \ldots, g_k\}$, $k \leq n$, a test set for the group G if, whenever $\varphi(g_i) = g_i$, $i = 1, \ldots, k$, for some endomorphism f of the group G, this φ is actually an automorphism of G. The test rank of G is the minimal cardinality of a test set.

A natural question now is (see [43, Problem (FP23)]): can the test rank of G be equal to 2 if $n > 2$? If G has a test element, the test rank of G is obviously 1. For example, any free group of finite rank has test rank 1. On the other hand, there are groups (for example, free abelian groups of finite rank) whose test rank equals their rank. (Obviously, it cannot be bigger than that.)

Timoshenko [382] proved that a free metabelian group of rank ≥ 3 has test rank 2. Rocca and Turner [316] have shown recently that for any pair of integers (k, n) with $1 \leq k \leq n$, there are finitely generated abelian groups of rank n and test rank k.

2.4 The "Double Jacobian" Matrix

In this section, we establish a direct connection between the "test element" approach to recognizing automorphisms and the "inverse function theorem" due to Birman [54] (see our Section 1.4).

We define for any element $u \in F_n$ the "double Jacobian" matrix $D_u = (d_i'(d_j(u)))_{1\le i,j\le n}$, where d_j is the "usual", or left, Fox derivation and d_i' is the right Fox derivation (see Section 1.4). Then:

Theorem 2.4.1. *Let φ be an endomorphism of the group F. It is an automorphism*

(i) *if and only if the matrix $D_{\varphi(u)}$ is invertible over $\mathbb{Z}F$ with $u = [x_1, x_2]\dots[x_{n-1}, x_n]$, n even;*

(ii) *if and only if the natural image over $\mathbb{Z}_2F$ of the matrix $D_{\varphi(u)}$ is invertible over $\mathbb{Z}_2F$ with $u = x_1^2x_2^2\dots x_n^2$.*

Proof. (i) Let $\varphi(x_i) = y_i$, $1 \le i \le n$, $n = 2m$, and let $v = \varphi(u)$. Apply a left Fox derivation d_j to both sides of this equality; by Lemma 1.4.5, this gives

$$d_j(u) = \sum_{1\le k\le n} \varphi(d_k(u))d_j(y_k). \tag{2.5}$$

Note that every $\varphi(d_k(u))$ has augmentation 0 since u belongs to the commutator subgroup F' so that $d_k(u) \in \Delta$, $1 \le k \le n$. Applying now a right Fox derivation d_i' to both sides of (2.5), we get by Lemma 1.4.5

$$d_i'(d_j(v)) = \sum_{1\le k\le n}\sum_{1\le m\le n} d_i'(y_m)\varphi(d_m'(d_k(u)))d_j(y_k). \tag{2.6}$$

When i and j run through $\{1,\dots,n\}$, (2.6) becomes a system of n^2 equalities that can be written in the matrix form as

$$D_{\varphi(u)} = J_\varphi'\varphi(D_u)J_\varphi, \tag{2.7}$$

where $J_\varphi = (d_j(y_i))_{1\le i,j\le n}$ is the left Jacobian matrix of φ; $J_\varphi' = (d_i'(y_j))_{1\le i,j\le n}$ is the right Jacobian matrix of φ.

Suppose the matrix $D_{\varphi(u)}$ is invertible. Then every matrix on the right-hand side of (2.7) must be invertible, too, which implies φ is an automorphism by Birman's result.

Conversely, suppose φ is an automorphism. Then, again by Birman's theorem, the matrices J_φ' and J_φ are invertible (actually, the result of Birman applies to the matrix J_φ, but applying Lemma 1.4.7 immediately gives the same result for J_φ' as well). Now we have to consider the matrix D_u; it is a block-matrix having m 2×2 matrices B_k along the diagonal and zeros below; here

$$B_k = \begin{pmatrix} x_{2k-1}^{-1}x_{2k}^{-1}(x_{2k}-1) & 1 - x_{2k-1}^{-1}x_{2k}^{-1}(x_{2k-1}-1) \\ -x_{2k}^{-1} & x_{2k}^{-1} - x_{2k}^{-1}x_{2k-1} \end{pmatrix},$$

$1 \leq k \leq m$. It can be easily verified that every matrix B_k has the inverse

$$B_k^{-1} = \begin{pmatrix} x_{2k-1} - x_{2k-1}^2 & (1 - x_{2k-1})(x_{2k} - 1) - x_{2k} \\ x_{2k-1} & x_{2k-1} \end{pmatrix}.$$

Hence the matrix D_u is invertible, and so is the matrix $D_{\varphi(u)}$ on the left-hand side of (2.7). This completes the proof of part (i) of the theorem.

(ii) The proof goes along the same lines as that of part (i) upon replacing the group ring $\mathbb{Z}F$ with $\mathbb{Z}_2F$. On the right-hand side of (2.5), the elements $\varphi(d_k(u))$ will have augmentation 0 because, in the ring $\mathbb{Z}_2F$, one has $d_k(u) \in \Delta_F$ whenever $u \in F^2$. Then, Birman's theorem remains valid on replacing $\mathbb{Z}F$ with $\mathbb{Z}_2F$ (see Remark 1.4.9). Finally, for $u = x_1^2 x_2^2 \dots x_n^2$, the matrix D_u is an upper triangular matrix with the units on the diagonal; in particular, it is invertible over any ring, and this completes the proof. ■

It is easy to produce many examples of elements u of the group ring $\mathbb{Z}F$ with D_u invertible. However, in the group F itself, the only elements we know with this property are $[x_1, x_2] \dots [x_{n-1}, x_n]$, $x_1^2 x_2^2 \dots x_n^2$ and their automorphic images. We have to admit that we do not know what makes the double Jacobian matrix of an element $u \in F$ invertible. It is clear that if an element $u \in F$ has the matrix D_u invertible, then it is a test element for recognizing automorphisms; the converse, however, is not true. For example, elements of the form $x_1^p x_2^p \dots x_n^p$, $p \geq 3$, are test elements, but they have the double Jacobian matrix noninvertible.

Remark 2.4.2. If we switch left and right Fox derivatives in the definition of the double Jacobian matrix (i.e., put $D'_u = (d_i(d'_j(u)))_{1 \leq i,j \leq n}$), then D'_u turns out to be the transpose of D_u. In particular, Theorem 2.4.1 holds also on replacing $D_{\varphi(u)}$ with $D'_{\varphi(u)}$.

3
Other Special Elements

In this chapter, we consider various generalizations of primitive elements: *generic elements* in the sense of Stallings [375], *almost primitive elements* in the sense of Rosenberger [318], and Δ-primitive elements in the sense of Shpilrain [356]. It turns out that all these generalizations are related, but relations between them are rather nontrivial, which opens several interesting research avenues.

3.1 Δ-Primitive Elements

We start with Δ-primitive elements. These are defined by means of homological properties of the corresponding one-relator group. They make "nice" orbits under the action of the automorphism group of a free group and also have other interesting properties that bring together group theory, topology, and homological algebra.

As usual, let $F = F_n$ be the free group of a finite rank $n \geq 2$ with a set $X = \{x_1, \ldots, x_n\}$ of free generators.

Definition 3.1.1 ([356]). Let J be a right ideal of the free group ring $\mathbb{Z}F$. An element $u \in F$ is called J-primitive if Fox derivatives (see Section 1.4) of the element u generate J as a right ideal of $\mathbb{Z}F$.

Now "usual" primitive elements are the same as $\mathbb{Z}F$-primitive ones — this nontrivial fact follows from a matrix characterization of primitive elements given by Umirbaev [389] (see also [95, Corollary IV.5.3]).

We focus here on Δ-primitive elements of a free group F, where Δ is the augmentation ideal of $\mathbb{Z}F$. Another motivation for considering Δ-primitive elements comes from commutative algebra. We recall some facts here very briefly. A vector $(p_1, \ldots, p_m)$ of (Laurent) polynomials is called *unimodular* if $p_1, \ldots, p_m$ generate the whole (Laurent) polynomial algebra P as an ideal. Then, a vector $(p_1, \ldots, p_m)$ of Laurent polynomials is called Δ-*modular* (see [20]) if $p_1, \ldots, p_m$ generate the augmentation ideal Δ as an ideal of the whole algebra. Suslin [379] and Artamonov [20] have proved that the group $\mathrm{GL}_m(P)$, $m \geq 3$, acts transitively on the set of all unimodular and all Δ-modular vectors, respectively.

Now the result of Umirbaev cited above can be considered a free group analog of Suslin's result: it says that the group $\mathrm{Aut}(F)$ acts transitively on the set of all $\mathbb{Z}F$-primitive elements (i.e., of those with a unimodular vector of Fox derivatives).

The desire to get a free group analog of Artamonov's result draws our attention to Δ-primitive elements. First we note that one can give an equivalent definition of Δ-primitivity using a different language: an element $u \in F$ is Δ-primitive if and only if the cohomology group $H^2(G, \mathbb{Z}G)$, when regarded as a G-module (with G-action induced by the right regular action on $\mathbb{Z}G$), is isomorphic to the trivial G-module $\mathbb{Z}$, where G is a one-relator group $\langle F \mid u \rangle$.

If the group F has an even rank $n = 2m$, then the element

$$u_n = [x_1, x_2][x_3, x_4] \ldots [x_{n-1}, x_n]$$

is Δ-primitive (and hence so is every element from $\mathrm{Orb}_{\mathrm{Aut}(F)}(u_n)$). On the other hand, a free group of an odd rank has no Δ-primitive elements whatsoever — see Corollary 3.1.6 below. R. Bieri has pointed out to us that a combination of results of [53], [117], and [417] yields the following:

Theorem 3.1.2. *In a group F_{2m}, $m \geq 1$, any Δ-primitive element is an automorphic image of $u_{2m} = [x_1, x_2][x_3, x_4] \ldots [x_{2m-1}, x_{2m}]$.*

This, together with Corollary 3.1.6 below, gives a free group analog of Artamonov's result:

Corollary 3.1.3. *In a free group F of finite rank, the group $\mathrm{Aut}(F)$ acts transitively on the set of all Δ-primitive elements.*

In the case of F_2, Theorem 3.1.2 yields an explicit combinatorial description of Δ-primitive elements since every automorphic image of $[x_1, x_2]$ in the group F_2 has the form $[x_1, x_2]^g$ or $[x_2, x_1]^g$ for some $g \in F_2$. Note that there is also an explicit combinatorial description of $\mathbb{Z}F_2$-primitive elements due to [71] (see also [296]).

There is also a nice matrix characterization of Δ-primitive elements:

Proposition 3.1.4.

(i) *An element* $u \in [F_n, F_n]$ *is* Δ*-primitive if and only if the matrix* $D_u = (d'_j(d_i(u)))_{1 \le i,j \le n}$ *is invertible over the ring* $\mathbb{Z}F_n$.

(ii) *If* φ *takes a* Δ*-primitive element of the group* F_n *to another* Δ*-primitive element, then* φ *is an automorphism.*

The matrix D_u (the "double Jacobian" matrix) was introduced in [355] (see also our Section 2.4). Here d'_j denotes the right partial Fox derivation with respect to x_j, whereas d_i is the "usual", left Fox derivation — see Section 1.4.

We also treat the case of a free metabelian group $M_n = F_n/F_n''$ to obtain Corollary 3.1.6 below. (In the definition of a Δ-primitive element in M_n, we consider abelianized Fox derivatives.)

Theorem 3.1.5.

(i) *The group* $\mathrm{Aut}(M_2)$ *acts transitively on the set of all* Δ*-primitive elements of* M_2. *More specifically, every* Δ*-primitive element of* M_2 *is an automorphic image of the element* $[x_1, x_2]$ *and therefore has the form* $[x_1, x_2]^g$ *or* $[x_2, x_1]^g$ *for some* $g \in M_2$.

(ii) *There are no* Δ*-primitive elements in the group* M_n *if* n *is odd.*

Corollary 3.1.6. *There are no* Δ*-primitive elements in the free group* F_n *if* n *is odd.*

Talking about a general case of J-primitive elements for an arbitrary right ideal J of the group ring $\mathbb{Z}F$, we note first of all that J-primitive elements do not always exist. For example, if J cannot be generated by less than $(n+1)$ elements, then there are obviously no J-primitive elements in the group F_n. In fact, if g is a J-primitive element and the ideal J is k-generated, then g has *outer rank* k in the sense defined in [352] (the minimum number of free generators on which an automorphic image of g can depend). This follows from a result of Umirbaev [391].

Deciding for which (right) ideals J of the group ring $\mathbb{Z}F$ the group $\mathrm{Aut}(F)$ acts transitively on the set of all J-primitive elements of F seems to be a difficult problem. Actually, it makes sense only for *characteristic* ideals (i.e., those invariant under free group automorphisms). Note that if an element $g \in F$ is J-primitive for a characteristic right ideal J, then every automorphic image of g is J-primitive, too.

Also, it is easy to show that for any m-generator right ideal J of $\mathbb{Z}F$, the group $\mathrm{GL}_m(\mathbb{Z}F)$ acts transitively on the set of all m-tuples of elements generating J.

Of particular interest are J-primitive elements of maximal outer rank $n = \mathrm{rank}\, F$ in the case where J is the right ideal generated by Fox derivatives of a single group element:

Proposition 3.1.7. *Let $g \in F_n$ be an element of outer rank n, and let J be the right ideal of $\mathbb{Z}F_n$ generated by Fox derivatives of g. If a* monomorphism *(i.e., injective endomorphism) φ of the group F_n takes g to another J-primitive element, then φ is actually an automorphism.*

In particular:

Corollary 3.1.8 (see [383]). *Let $g \in F_n$ be an element of outer rank n. If $\varphi(g) = g$ for some monomorphism φ of the group F_n, then φ is actually an automorphism.*

Now we get to the proofs of the results of this section.

Lemma 3.1.9. *Let J be a right ideal of $\mathbb{Z}F$ (hence a free right module over $\mathbb{Z}F$) generated as a free module over $\mathbb{Z}F$ by $u_1, \ldots, u_m$. Then the following conditions are equivalent:*

(a) *A matrix $M = (a_{ij})_{1 \le i,j \le m}$ is invertible over $\mathbb{Z}F$ (i.e., $M \in \mathrm{GL}_m(\mathbb{Z}F)$);*

(b) *The elements $y_j = \sum_{k=1}^{m} (u_k - 1) a_{kj}$, $1 \le j \le m$, generate the ideal J as a right ideal of $\mathbb{Z}F$.*

Proof. Suppose M is invertible over $\mathbb{Z}F$; denote by U the row matrix $(u_1, \ldots, u_m)$ and by Y the row matrix $(y_1, \ldots, y_m)$. Then $UMM^{-1} = YM^{-1} = U$, which means that $u_1, \ldots, u_m$ belong to the right ideal of $\mathbb{Z}F$ generated by $y_1, \ldots, y_m$. Conversely, suppose we have $YB = U$ for some matrix B over $\mathbb{Z}F$. Then $UMB = U$, and hence $MB = I$, the identity matrix, because $(u_1, \ldots, u_m)$ form a free basis of a free right $\mathbb{Z}F$-module J. This implies $M \in \mathrm{GL}_m(\mathbb{Z}F)$ — see, e.g., [80]. ■

Before we get to a proof of Theorem 3.1.2, we consider a couple of examples.

Example 3.1.10. The element $u = [x_1, x_2][x_3, x_4] \ldots [x_{2m-1}, x_{2m}]$ of the group F_{2m} is Δ-primitive since the corresponding double Jacobian matrix D_u is invertible — see our Section 2.4.

Example 3.1.11. The element $v = [x_1, x_2][x_2, x_3][x_3, x_4]$ of the group F_4 is Δ-primitive. It is not quite obvious that v is an automorphic image of $u = [x_1, x_2][x_3, x_4]$. However, this is the case: u is taken to v by the following automorphism: $x_1 \to x_1 x_3^{-1}$; $x_2 \to x_3 x_2 x_3^{-1}$; $x_3 \to x_3$; $x_4 \to x_4$.

Proof of Theorem 3.1.2. We give a proof here without introducing background material, just referring to [53] and [117] for details.

First of all, it is an immediate consequence of the definition that $g \in F$ is a Δ-primitive element if and only if for the right ideal J_g of the group ring $\mathbb{Z}F$ generated by Fox derivatives of u one has the factor-module $\mathbb{Z}F/J_g$ isomorphic to the trivial F-module $\mathbb{Z}$. In other words, as we have mentioned before, the cohomology group $H^2(G, \mathbb{Z}G)$ of the one-relator group $G =$

$\langle F \mid g \rangle$ is infinite cyclic. It is also clear that the group G is torsion-free for if it was not, the element g would be a proper power, and such an element could not be Δ-primitive since the augmentations of its Fox derivatives would have a nontrivial common divisor.

Then, Theorem 9.3 of [53] implies that the group $\langle F \mid g \rangle$ is a *Poincaré duality group of dimension* 2 (PD^2-group). It has been proved in [117] that every one-relator (torsion-free) PD^2-group is a surface group.

Applying now a result of Zieschang [417], we see that, when $F = F_{2m}$, g must be an automorphic image of $u_{2m} = [x_1, x_2][x_3, x_4] \dots [x_{2m-1}, x_{2m}]$. This completes the proof. ∎

Proof of Proposition 3.1.4.

(i) First suppose the matrix $D_u = (d'_j(d_i(u)))_{1 \le i,j \le n}$ is invertible. Then, by Lemma 3.1.9, the elements $y_i = \sum_{k=1}^{n}(x_k - 1)d'_k(d_i(u)) = d_i(u) - \varepsilon(d_i(u))$, $1 \le i \le n$, generate the ideal Δ as a right ideal of $\mathbb{Z}F$. Since $u \in F'$, we have $\varepsilon(d_i(u)) = 0$, $1 \le i \le n$, by Lemmas 1.4.1 and 1.4.2. Therefore, u is Δ-primitive.

Conversely, if u is Δ-primitive, then the elements $d_i(u) = \sum_{k=1}^{n}(x_k - 1)d'_k(d_i(u))$ generate Δ as a right ideal of $\mathbb{Z}F$. Again by Lemma 3.1.9, the matrix D_u is invertible.

(ii) We use an argument from [355] implying that if a matrix $D_{\varphi(u)}$ is invertible and $u \in F'$, then φ is an automorphism. Applying part (i) of this proposition completes the proof. ∎

Proof of Theorem 3.1.5. First of all, note that if u is Δ-primitive, then $u \in M'$; otherwise some $d_i(u)$ wouldn't belong to Δ by Lemmas 1.4.1 and 1.4.2.

(i) Let $h \in M'_2$; then we can write h as $[x_1, x_2]^w$ for some $w \in \mathbb{Z}A_2 = \mathbb{Z}(M_2/M'_2)$. Then, for abelianized Fox derivatives (we denote them the same way as the ones in a free group ring when there is no ambiguity) we have $d_i(h) = w \cdot d_i([x_1, x_2])$. Hence, if $d_i(h)$, $i = 1, 2$, and generate the same ideal of $\mathbb{Z}A_2$ as $d_i([x_1, x_2])$, the element w should be invertible in $\mathbb{Z}A_2$, which means it has the form $\pm g$ for some $g \in M_2/M'_2$.

Thus $h = [x_1, x_2]^{\pm g}$; in particular, h is an automorphic image of $[x_1, x_2]$.

(ii) Consider basic commutators of weight 2 in the group M_n: $c_1 = [x_1, x_2]$, $c_2 = [x_1, x_3], \dots$, $c_N = [x_{n-1}, x_n]$, where $N = n(n-1)/2$, and consider a product of the form $w = c_1^{k_1} c_2^{k_2} \dots c_N^{k_N}$. Evaluate abelianized Fox derivatives of the element w:

$$d_1(w) = k_1(x_2 - 1) + \dots + k_{n-1}(x_n - 1);$$
$$d_2(w) = -k_1(x_1 - 1) + k_n(x_3 - 1) + \dots + k_{2n-3}(x_n - 1);$$
$$d_3(w) = -k_2(x_1 - 1) - k_n(x_2 - 1) + k_{2n-2}(x_4 - 1) + \dots + k_{3n-6}(x_n - 1);$$

$$\dots$$

$$d_n(w) = -k_{n-1}(x_1 - 1) - \dots - k_{n(n-1)/2}(x_{n-1} - 1).$$

We are now going to show that these derivatives do not generate Δ even modulo Δ^2. To do that, it suffices to show that they are linearly dependent; i.e., that the $n \times n$ matrix of coefficients (its (i,j)th entry is the coefficient at $(x_j - 1)$ in the decomposition of $d_i(w)$ above) has determinant 0.

It is easy to see that this matrix (denote it by $A = (a_{ij})$) is antisymmetric, with zeros on the diagonal. The determinant of a matrix like that must be 0 if n is odd. Indeed, consider a summand $a_{1,i_1}a_{2,i_2}\dots a_{n,i_n}$ in the decomposition of the determinant. If there is at least one diagonal element among these a_{k,i_k}, then the product is 0. If all a_{k,i_k} are off-diagonal elements, consider the "reflection" $a_{i_1,1}a_{i_2,2}\dots a_{i_n,n}$. These two summands go with different signs since $a_{ij} = -a_{ji}$ and n is odd. Therefore, they cancel out, which proves that the determinant of A equals 0. This completes the proof of part (ii). ■

Proof of Corollary 3.1.6. If there were a Δ-primitive element in F_n, its image in M_n would be a Δ-primitive element of M_n, which contradicts Theorem 3.1.5 (ii). ■

Proof of Proposition 3.1.7. Let $h = \varphi(g)$ be a J-primitive element. Since g has outer rank n, the right ideal J is n-generated by [391]. It follows that the elements $d_1(g),\dots,d_n(g)$ freely generate J as a right ideal of $\mathbb{Z}F_n$. Indeed, if there were a (right) $\mathbb{Z}F_n$-dependence between these elements, then one of them would belong to the right ideal generated by the others — this follows from a general theory of [80]. Therefore, J could be generated by less than n elements.

Thus, by Lemma 3.1.9, for some matrix $M \in \mathrm{GL}_n(\mathbb{Z}F_n)$, we have

$$(d_1(h),\dots,d_n(h)) = (d_1(g),\dots,d_n(g))M. \tag{3.1}$$

On the other hand, by the "chain rule", we have

$$(d_1(h),\dots,d_n(h)) = (\varphi(d_1(g)),\dots,\varphi(d_n(g)))J_\varphi.$$

This together with (3.1) gives

$$(d_1(g),\dots,d_n(g)) = (\varphi(d_1(g)),\dots,\varphi(d_n(g)))J_\varphi M^{-1}. \tag{3.2}$$

This means $J \subseteq \varphi(J)$. Suppose $J \subset \varphi(J)$ (i.e., $J \neq \varphi(J)$). Since φ is a monomorphism, this implies $\varphi^k(J) \subset \varphi^{k+1}(J)$ for any $k \geq 1$ so that we have an infinite ascending chain of n-generated right ideals

$$J \subset \varphi(J) \subset \varphi^2(J) \subset \dots, \tag{3.3}$$

which is impossible. Indeed, suppose we have two n-generated right ideals J_1 and J_2 with (free) bases $\{a_1,\dots,a_n\}$ and $\{b_1,\dots,b_n\}$, respectively, and suppose that $J_2 \subset J_1$. We can assume that the base of J_1 is *reduced* in the following sense. The free group ring $\mathbb{Z}F$ is known to be graded (see, e.g., [80]), so we can consider the *leading part* (or the leading monomial) $\tilde{a}_i$ of every a_i with respect to this grading. Now we say that our base is reduced if $\tilde{a}_i = \tilde{a}_j \cdot u$ for some $u \in \mathbb{Z}F$ implies $i = j$.

If our base was not reduced, we could reduce it in a finite number of steps upon replacing a_i with $a_i - a_j \cdot u$ every time we have $\tilde{a}_i = \tilde{a}_j \cdot u$, $i \neq j$.

Thus, we assume that the base of J_1 is reduced, and then we see that since every b_i is of the form $\sum_{i=1}^{n} a_i \cdot v_i$, the sum of weights of the leading parts $\tilde{b}_i$ of all b_i is no smaller than that of the leading parts of a_i (here we use the fact that in a free ideal ring one cannot have $a_i \cdot u = a_j \cdot v$ unless $a_i \cdot u = a_j$ or $a_i = a_j \cdot v$ — see [80]).

Since we can have only finitely many different right ideals whose bases have a given sum of weights of the leading parts of their elements, this proves that (4) is impossible.

Thus, we should actually have $J = \varphi(J)$, in which case the matrix $J_\varphi M^{-1}$ on the right-hand side of (3.2) must be invertible by Lemma 3.1.9. Therefore, J_φ is invertible, too, and hence $\varphi \in \mathrm{Aut}(F_n)$ by [54]. ■

Corollary 3.1.8 follows immediately.

3.2 Almost Primitive and Generic Elements

Our exposition here follows [132].

Definition 3.2.1 ([132]). An *almost primitive element* (APE) is an element of a free group F that is not primitive in F but is primitive in any proper subgroup of F containing it.

This can be extended to arbitrary groups in the following manner. An element $g \in G$ is *primitive* in G if g generates an infinite cyclic free factor of G; i.e., g has infinite order and $G = \langle g \rangle * G_1$ for some $G_1 \subset G$. g is then an APE if it is not primitive in G but primitive in any proper subgroup containing g. Rosenberger [319] proved that in the free group $F = F(x_i, y_i, z_j)$, $1 \leq i \leq m$, $1 \leq j \leq n$, of rank $2m + n$, the element

$$[x_1, y_1] \dots [x_m, y_m] z_1^{p_1} \dots z_n^{p_n},$$

where the p_i are not necessarily distinct primes, is an APE in F. Rosenberger [319] also proved, in a different setting, that if A, B are arbitrary groups containing APEs a, b, respectively, then the product ab is either primitive or an APE in the free product $A * B$. This was reproven by Brunner, Burns, and Oates-Williams [60], who also prove the more difficult result that if a and b are tame APEs in groups A, B, respectively, then their product normally is a tame APE in $A * B$. An APE w in a group G is a *tame APE* if whenever $w^\alpha \in H \subset G$ with $\alpha \geq 1$ minimal, then either w^α is primitive in H or the index $[G : H]$ is α. It follows easily that $[a_1, b_1] \dots [a_g, b_g]$, $g \geq 1$, is a tame APE in the free group on $a_1, b_1, \dots, a_g, b_g$. We note that Brunner, Burns, and Oates-Williams give a more technical definition of a tame APE.

Definition 3.2.2. Let $\mathcal{U}$ be a variety defined by a set of laws $\mathcal{V}$. (We refer to the book of H. Neumann [291] for relevant terminology.) For a group G, we let $\mathcal{V}(G)$ denote the verbal subgroup of G defined by $\mathcal{V}$. An element $g \in G$ is *$\mathcal{U}$-generic* in G if $g \in \mathcal{V}(G)$ and whenever H is a group, $f\colon H \to G$ a homomorphism, and $w = f(u)$ for some $u \in \mathcal{V}(H)$, it follows that f is surjective. Equivalently, $g \in G$ is $\mathcal{U}$-generic in G if $g \in \mathcal{V}(G) \subset G$ but $g \notin \mathcal{V}(K)$ for every proper subgroup K of G [375]. An element is *generic* if it is $\mathcal{U}$-generic for some variety $\mathcal{U}$.

For $n = 0$ we have $\mathcal{U}_n = \mathcal{A}$, the abelian variety. Stallings [375] and Dold [100] have given sufficient conditions for an element of a free group to be $\mathcal{U}_n$-generic. Using this, it can be shown that $x_1^n x_2^n \dots x_m^n$ is $\mathcal{U}_n$-generic in the free group on $x_1, \dots, x_m$ for all $n \geq 2$, and if m is even, then $[x_1, x_2] \dots [x_{m-1}, x_m]$ is $\mathcal{U}_n$-generic in the free group on $x_1, \dots, x_m$ for $n = 0$ and for all $n \geq 2$. These facts are also consequences of a result of Rosenberger [318].

Comerford [82] points out that if G is Hopfian, which is the case if G is free, then being generic implies being a test word (see our Chapter 2). Thus, for free groups we have

$$\text{generic} \longrightarrow \text{test word}.$$

Comerford also shows that there is no converse. In particular, he shows that in a free group of rank 3 on x, y, z the word $w = x^2[y^2, z]$ is a test word but is not generic. We can also show that, in general, generic does not imply APE. Suppose $F = F(x, y)$ is the free group of rank 2 on x, y, and let $w = x^4 y^4$. Then w is $\mathcal{U}_4$-generic but w is not an APE since $w \in \langle x^2, y^2 \rangle$ and is not primitive in this subgroup while this subgroup is not all of F.

Further, in general it is not true that being an APE implies being a test word. Again let $F = F(x, y)$ and let $w = x^2 y x^{-1} y^{-1}$. Brunner, Burns, and Oates-Williams show that w is an APE. However, Turner [383] shows that w is not a test word. Since generic elements are test words in a Hopfian group, this example shows further that APE does not imply generic in general. This is really to be expected since test words are strongly nonprimitive. However, Theorem 3.2.3 below shows that many APEs are indeed generic and therefore test words.

Recall that a variety $\mathcal{U}$ defined by the set of laws $\mathcal{V}$ is a nontrivial variety if it consists of more than just the trivial group. In this case $\mathcal{V}(F) \neq F$ for any free group F.

Theorem 3.2.3. *Let F be a free group and $\mathcal{B}$ a nontrivial variety defined by the set of laws $\mathcal{V}$. Let $w \in \mathcal{V}(F)$. If w is an APE, then w is $\mathcal{B}$-generic. In particular, w is a test word.*

Proof. Let $w \in \mathcal{V}(F)$ be an APE and let $\varphi\colon H \to F$ be a homomorphism with $\varphi(u) = w$ for some $u \in \mathcal{V}(H)$. As in the statement of the theorem, $\mathcal{V}$ is the set of laws defining the nontrivial variety $\mathcal{B}$. Let K be a proper subgroup

of F. If $w \notin K$, then clearly $w \notin \mathcal{V}(K)$. If $w \in K$, then since w is an APE, w is primitive in K since K is a proper subgroup of F. Furthermore, since $\mathcal{B}$ is a nontrivial variety and K is free, we have that $K \neq \mathcal{V}(K)$. It follows then from the primitivity of w in K that $w \notin \mathcal{V}(K)$. Therefore $w \in \mathcal{V}(F)$ and for any proper subgroup K of F we have $w \notin \mathcal{V}(K)$ and hence w is $\mathcal{B}$-generic. Since free groups are Hopfian, w must then be a test word. ■

In particular, let $F(n)$ be the subgroup of the free group F generated by all commutators and nth powers, $n \geq 2$ or $n = 0$; that is, $F(n) = \mathcal{V}_n(F)$. Then:

Corollary 3.2.4. *Let $w \in F(n)$ with $n \geq 2$ or $n = 0$. If w is an APE, then w is $\mathcal{U}_n$-generic and w is a test word.*

Now we give, without a proof, a class of examples of generic elements in F_2. We refer to [132] for details.

Theorem 3.2.5. *Let F be a free group on a, b and let $X = \langle x_1, \ldots, x_k \rangle$, $k \geq 1$, be a finitely generated subgroup of F. Suppose that X contains the element $[a^n, b^m]$ for positive integers n, m. Then $\{x_1, \ldots, x_k\}$ can be carried by Nielsen transformations into a free basis $\{y_1, \ldots, y_p\}$, $1 \leq p \leq k$, for which one of the following cases occurs.*

(1) $y_1 = [a_n, b_m]$ *is a primitive element of X;*

(2) $y_1 = a^\alpha$, $1 \leq \alpha \leq n$, $\alpha | n$ *and*
$y_2 = b^\beta$, $1 \leq \beta \leq m$, $\beta | m$;

(3) $y_1 = a^\alpha$, $1 \leq \alpha \leq n$, $\alpha | n$ *and*
$y_2 = b^m a^\beta b^{-m}$, $1 \leq \beta \leq n$, $\beta | n$;

(4) $y_1 = b^\alpha$, $1 \leq \alpha \leq m$, $\alpha | m$ *and*
$y_2 = a^n b^\beta a^{-n}$, $1 \leq \beta \leq m$, $\beta | m$;

(5) $y_1 = a^\alpha$, $1 \leq \alpha \leq n$, $\alpha | n$ *and*
$y_2 = b^m a^\beta$, $1 \leq \beta < \alpha$;

(6) $y_1 = b^\alpha$, $1 \leq \alpha \leq m$, $\alpha | m$ *and*
$y_2 = a^n b^\beta$, $1 \leq \beta < \alpha$;

(7) $y_1 = a^n b^m$, $y_2 = a^\alpha$, $1 \leq \alpha \leq 2n$, $\alpha | 2n$ *and*
$y_3 = b^\beta$, $1 \leq \beta \leq 2m$, $\beta | 2m$.

Using this theorem, we obtain the following corollaries.

Recall that $\mathcal{U}_n$ is the variety generated by the laws $\mathcal{V}_n = \{[x, y], z^n\}$, $n = 0$, or $n \geq 2$. We let $\mathcal{L}_n$ be the variety generated by the laws $\mathcal{W}_n = \{[x^n, y^n]\}$, $n \geq 1$. We then obtain the following class of generic elements.

Corollary 3.2.6. *Let F be a free group of rank 2 on x, y. Then $[x^n, y^n]$ is $\mathcal{L}_n$-generic in F, but for $n \geq 2$ it is not $\mathcal{U}_n$-generic in F.*

Corollary 3.2.7. *Let F be a free group of rank 2 on x, y. Then the element $[x^n, y^m]$, $n, m \geq 1$, is an APE if and only if $n = m = 1$.*

Recall that in general it is not true that being an APE implies being a test word. As mentioned earlier, if $F = F(x, y)$ and $w = x^2yx^{-1}y^{-1}$, then w is an APE but is not a test word. Since generic elements are test words, this example shows further that APE does not imply generic in general. However, using the same techniques as in Theorem 3.2.5, we can generalize the fact that the element w above is an APE to obtain further examples of APEs and test words.

Theorem 3.2.8. *Let $F = \langle a, b; \rangle$ and let $X = \langle x_1, \ldots, x_k \rangle \subset F$, $k \geq 1$. Suppose $a^n b a^{-1} b^{-1} \in X$, $n \geq 2$. Then $\{x_1, \ldots, x_k\}$ can be carried by Nielsen transformations into a free basis $\{y_1, \ldots, y_p\}$, $1 \leq p \leq k$, of X such that one of the following cases holds:*

(1) $y_1 = a^n b a^{-1} b^{-1}$ *or*

(2) $y_1 = a$, $y_2 = b$.

From this theorem and Theorem 3.2.3, we get the following corollary:

Corollary 3.2.9. *Let $F = \langle a, b; \rangle$. Then*

(1) $a^n b a^{-1} b^{-1}$, $n \geq 2$, *is an APE;*

(2) $a^n b a^{-1} b^{-1}$, $n \geq 3$, *is $\mathcal{U}_{n-1}$-generic.*

4
Automorphic Orbits

Automorphic orbits in a free group F_n of finite rank are sets of the form $\mathrm{Orb}_{\mathrm{Aut}\,F_n}(u) = \{v \in F_n,\ v = \varphi(u) \text{ for some } \varphi \in \mathrm{Aut}(F_n) \text{ and a fixed } u \in F_n\}$. One special and very interesting automorphic orbit is the set of all *primitive elements* (these are automorphic images of a free generator of F_n). In particular, the following problem, along with its generalizations [352], has been a source of inspiration for several people:

Problem 4.0.1 ([352, 43]). If an endomorphism φ of a free group F_n takes every primitive element to another primitive, is φ an automorphism?

Recently, D. Lee [205] has settled this problem in the affirmative for every n. Then, in [206], she settled a more general problem:

Problem 4.0.2 ([352]). If an endomorphism φ of F_n preserves an automorphic orbit $\mathrm{Orb}_{\mathrm{Aut}\,F_n}(u)$, $u \neq 1$; i.e., if φ acts "like an automorphism" on one particular orbit, then is φ itself an automorphism?

We refer to the original paper [205] for a rather lengthy argument that settles Problem 4.0.1 and reproduce below, in Section 4.3, an elegant argument that settles Problem 4.0.2.

Other interesting problems arise from considering "abridged" orbits $\{v \in F_n;\ |v| = |u|,\ \varphi(v) = u \text{ for some } \varphi \in \mathrm{Aut}(F_n)\}$. For instance, the problem of counting primitive elements of a given length (see Problem (F17) in [43]) has received considerable attention lately.

Another interesting (and important) problem is the following:

Problem 4.0.3 ([43]). Let u be an element of the free group F_n whose length $|u|$ cannot be decreased by any automorphism of F_n. Let $A(u)$ denote the set of elements $\{v \in F_n;\ |v| = |u|,\ f(v) = u \text{ for some } f \in \mathrm{Aut}(F_n)\}$. How fast does the cardinality of $A(u)$ grow as a function of $|u|$?

The set $A(u)$ is therefore an "abridged" orbit $\mathrm{Orb}_{\mathrm{Aut}(F_n)}(u)$ that includes only those automorphic images of u that have the same length as u does.

Problem 4.0.3 was motivated by complexity issues for Whitehead's algorithm that determines whether or not a given element of a free group of finite rank is an automorphic image of another given element. We address this problem in Section 4.2.2.

4.1 Finite Orbits

In this section, we give a description of finite automorphic orbits. Our exposition here follows [286].

Let F_n be the free group of a finite rank $n \geq 2$ with a set $X = \{x_i\}$, $1 \leq i \leq n$, of free generators. Denote by $\mathrm{Orb}_\varphi(u)$ the orbit of an element u of the free group F_n under the action of an automorphism φ. That is, $\mathrm{Orb}_\varphi(u) = \{v \in F_n,\ v = \varphi^m(u) \text{ for some } m \in \mathbb{Z}_+\}$.

The problem that we address in this section is: how many elements can a *finite* orbit like that possibly have if u runs through the whole group F_n and φ runs through the whole group $\mathrm{Aut}(F_n)$? The answer is provided by the following theorem, in combination with a result of McCool [240] (see also [179]):

Theorem 4.1.1. *In the free group F_n, there is an orbit $\mathrm{Orb}_\varphi(u)$ of cardinality k if and only if there is an element of order k in the group $\mathrm{Aut}(F_n)$.*

Thus, the question above is reduced to another question, that of finding out what possible order a torsion element of the group $\mathrm{Aut}(F_n)$ can have. The latter was answered by McCool [240]; more general results were obtained later by Khramtsov [179]. We cite the relevant result after the proof of Theorem 4.1.1.

It should be pointed out that the "only if" part of our Theorem 4.1.1 is no longer valid if φ is an arbitrary endomorphism. The following example is based on the idea suggested by C. Sims.

Example 4.1.2. In the free group F_3, let φ be the endomorphism that takes x_1 to $x_2^{-1}x_3$, x_2 to x_1, and x_3 to 1. Let $u = x_1x_2x_3$; then the cardinality of $\mathrm{Orb}_\varphi(u)$ is 5, but there is no element of order 5 in the group $\mathrm{Aut}(F_3)$.

Proof of Theorem 4.1.1.

(1) The "only if" part is a combination of an observation due to G. Levitt (see [211]) with a result of Bestvina and Handel [51]. Here is the argument. Suppose that, for some automorphism φ of the group F_n, one has $\varphi^k(g) = g$ and $\varphi^q(g) \neq g$ for $0 < q < k$.

Consider the action of φ on the subgroup $H = \mathrm{Fix}(\varphi^k)$ of all elements fixed by φ^k. (This subgroup is clearly invariant under φ since $\varphi^k(\varphi(h)) = \varphi(\varphi^k(h)) = \varphi(h)$.) Then φ is an automorphism of H. Indeed, φ is obviously surjective on H since, for any $h \in H$, we have $h = \varphi(\varphi^{k-1}(h))$. If φ were not injective on H, then we would have $\varphi(h) = 1$ for some $h \in H$, in which case h could not be fixed by φ^k.

Finally, φ clearly has order k as an element of the automorphism group $\mathrm{Aut}(H)$. Since H has rank at most n by [51], this yields the "only if" part of the theorem.

(2) To prove the "if" part, we need the following definition. A group G satisfies the *big powers* condition if, for any tuple of elements $u_1, \ldots, u_n$ from G with $[u_i, u_{i+1}] \neq 1$ $(i = 1, \ldots, n-1)$, there is an integer K such that for any integers $M_1, \ldots, M_n \geq K$, the following inequality holds:

$$u_1^{M_1} \ldots u_n^{M_n} \neq 1.$$

It is known that every free group satisfies the big powers condition [40]. Now comes the following:

Lemma 4.1.3. *Let φ be a nonidentical automorphism of F_n. Then there exists an integer $K \geq 1$ such that for any $M_1, \ldots, M_n \geq K$ the following inequality holds:*

$$\varphi(x_1^{M_1} \ldots x_n^{M_n}) \neq x_1^{M_1} \ldots x_n^{M_n}.$$

Proof. Suppose, by way of contradiction, that for any integer $K > 0$ there are integers $M_1(K), \ldots, M_n(K) \geq K$ such that

$$\varphi(x_1^{M_1(K)} \ldots x_n^{M_n(K)}) = x_1^{M_1(K)} \ldots x_n^{M_n(K)}.$$

It follows that

$$\varphi(x_1)^{M_1(K)} \ldots \varphi(x_n)^{M_n(K)} x_n^{-M_n(K)} \ldots x_1^{-M_1(K)} = 1 \qquad (4.1)$$

for all positive integers K. As we have mentioned above, the free group F_n satisfies the big powers condition; therefore there are two commuting consecutive factors in (4.1). Since φ is an automorphism, the only consecutive factors that can possibly commute are $\varphi(x_n)^{M_n(K)}$ and $x_n^{M_n(K)}$. It follows that $\varphi(x_n) = x_n$ and (4.1) takes the form

$$\varphi(x_1)^{M_1(K)} \ldots \varphi(x_{n-1})^{M_{n-1}(K)} x_{n-1}^{-M_{n-1}(K)} \ldots x_1^{-M_1(K)} = 1.$$

Upon repeating the argument above, we get $\varphi(x_i) = x_i$ for all $i = 1, \ldots, n$; i.e., φ is identical. This contradiction proves the lemma. ■

We now continue with our proof of the "if" part. Given $k > 1$ and an automorphism φ of order k of the group F_n, we are going to find an element $u \in F_n$ so that the orbit $\mathrm{Orb}_\varphi(u)$ has cardinality k.

If φ is a permutation on the set $\{x_1^{\pm 1}, \ldots, x_n^{\pm 1}\}$, then any element of the form $u = x_1^{M_1} \cdot \cdots \cdot x_n^{M_n}$, $M_i \neq 0$, would do. If not, then there is at least one free generator, say, x_1, such that $\varphi(x_1)$ has length at least 2. Let $u = x_1^{M_1} \cdot \cdots \cdot x_n^{M_n}$. Then, by Lemma 4.1.3, for some choice of $K \geq 1$, for any $M_1, \ldots, M_n \geq K$ we have $\varphi(u) \neq u$.

Similarly, for any m, $1 < m < k$, we can construct an element u_m such that $\varphi^m(u_m) \neq u_m$. Every u_m, $m \geq 2$, is chosen to be of the form $u_m = x_1^{M_{1,m}} \cdot \cdots \cdot x_n^{M_{n,m}}$ with $\min_i M_{i,m} > \max_i M_{i,m-1}$, and $\varphi^m(u_m) \neq u_m$ (the latter is possible by Lemma 4.1.3).

Obviously, with this choice of $M_{i,j}$ we will also have $\varphi^j(u_j) \neq u_j$ for any $j \leq m$. Therefore, for $u = u_k$, the orbit $\mathrm{Orb}_\varphi(u)$ will have cardinality k. ■

We note that possible values of the order of a torsion element of the group $\mathrm{Aut}(F_n)$ are described, according to [240] and [179], as follows. Pick a positive integer $k = p_1^{\alpha_1} \cdot \cdots \cdot p_s^{\alpha_s}$, where $p_1, \ldots, p_s$ are different primes. There is an element of order k in the group $\mathrm{Aut}(F_n)$ if and only if $\sum_{i=1}^{s}(p_i^{\alpha_i} - p_i^{\alpha_{i-1}}) \leq n$. For example, if $k = 15 = 3 \cdot 5$, then the sum above becomes $(3-1)+(5-1) = 6$. Therefore, there is an automorphism of order 15 in the group $\mathrm{Aut}(F_n)$ for $n \geq 6$ but not for $n \leq 5$.

We also note that Levitt and Nicolas [210] proved that the *maximum* order (call it $H(n)$) of a torsion element of $\mathrm{Aut}(F_n)$ is the same as that of a torsion element of $\mathrm{GL}_n(\mathbb{Z})$, with the exception of $n = 2, 6$, and 12. They also established the asymptotics of this function by showing $\log H(n) \sim \sqrt{n \cdot \log n}$.

4.2 Abridged Orbits

In this section, we study "abridged" automorphic orbits

$$A(u) = \{v \in F_r;\ |v| = |u|,\ f(v) = u \text{ for some } f \in \mathrm{Aut}(F_r)\}.$$

One of the most interesting special cases is where $u = x_1$. In other words, $A(x_1)$ is the set of primitive elements of a given length in F_r.

4.2.1 Counting primitive elements

Let $P(r, n)$ be the number of primitive elements of length n in F_r. For $r = 2$, the number $P(2, n)$ grows like $(\sqrt{3})^n$; this follows from [63, Proposition 4.1], as observed by Rivin [315].

We also note that the *precise* number of *cyclically reduced* primitive elements of length n in F_2 was given in [286] (see Proposition 4.2.4 below);

this number has linear growth as a function of n. This case however is exceptional, and it is easy to see that if $r \geq 3$, then the growth of the number of primitive elements (cyclically reduced or not) is exponential, say, λ^n. The problem is therefore to determine λ (as a function of r).

It was shown in [63] that $\lambda \leq \mu(r) > 2r-2$, where $\mu(r) \to (2r-2)$ as $r \to \infty$. In [58], it was shown that $\lambda \leq 2r-2$. In both papers, crucial for the counting arguments was the fact that the Whitehead graph of any primitive element of length > 2 has either an isolated edge or a cut vertex, i.e., a vertex that, having been removed from the graph together with all incident edges, increases the number of connected components of the graph.

Here we again exploit this fact to sharpen the estimate for λ:

Theorem 4.2.1 ([358]). *If $r \geq 3$, then, for some constants c_1, c_2, one has $c_1 \cdot n \cdot (2r-3)^n \leq P(r,n) \leq c_2 \cdot \lambda^n$, where $\lambda = r-1+\sqrt{(r-1)^2-1} < 2r-2$.*

It seems that this estimate exhausts the potential of the "cut vertex" approach, and further improvements would require brand new ideas. As for the ultimate result, we make the following

Conjecture 4.2.2. If $r \geq 3$, then $P(r,n) = O(n \cdot (2r-3)^n)$.

We note that $n \cdot (2r-3)^n$ is (up to a factor that does not depend on n) the number of "obvious" primitive elements of length n having the form $u \cdot x_i^{\pm 1} \cdot v$, where u, v are arbitrary elements that do not depend on x_i. Thus, our conjecture says that, for $r \geq 3$, "most" primitive elements are of that form.

Our proof here uses a refined analysis of the Whitehead graph of a primitive element and a new ingredient, namely, systems of linear recurrence relations, which is described below. We believe this technique can be used for other counting problems in (free) groups as well.

The Whitehead graph $\mathrm{Wh}(u)$ of a word $u \in F_r$ is obtained as follows. The vertices of this graph correspond to the elements of the free generating set X and their inverses. For each occurrence of a subword $x_i x_j$ in the word u, there is an edge in $\mathrm{Wh}(u)$ that connects the vertex x_i to the vertex x_j^{-1}; if u has a subword $x_i x_j^{-1}$, then there is an edge connecting x_i to x_j, etc. There is one more edge (the external edge) included in the definition of the Whitehead graph: this is the edge that connects the vertex corresponding to the last letter of u to the vertex corresponding to the inverse of the first letter.

It was observed by Whitehead himself that the Whitehead graph of any primitive element of length > 2 has either an isolated edge or a cut vertex (i.e., a vertex that, having been removed from the graph together with all incident edges, increases the number of connected components of the graph).

Both [42] and [63] exploited this fact to get upper bounds for $P(r,n)$. Here we refine these upper bounds based on the following simple observation (see, e.g., [402, Exercise 5.7]):

Suppose a simple graph Γ has the property that any two vertices can be included in a simple circuit. Then Γ does not have a cut vertex.

Our strategy therefore will be to produce an upper bound for the number of elements $u \in F_r$ whose Whitehead graph (or, rather, an associated simple graph) does *not* have the property alluded to in the previous observation.

Our counting technique is best visualized by introducing the *Whitehead tree* $\mathrm{WT}(u)$ associated to the graph $\mathrm{Wh}(u)$. The Whitehead tree $\mathrm{WT}(u)$ is an infinite rooted labeled tree; the root is labeled 1, and a parent vertex at a level k labeled x_i is connected to a child vertex at the level $(k+1)$ labeled x_j if and only if there is an edge from the vertex x_i to the vertex x_j^{-1} in the graph $\mathrm{Wh}(u)$ (or, equivalently, if u has a subword $x_i x_j$).

Now the problem of finding the growth function of the tree $\mathrm{WT}(u)$ (i.e., counting elements at a level n as a function of n) can be translated into a system of (linear) recurrence relations as follows. Let j_n (resp. $\overline{j_n}$) be the number of vertices labeled x_j (resp. x_j^{-1}) at the level n of the tree $\mathrm{WT}(u)$. Then, based on the Whitehead graph $\mathrm{Wh}(u)$, it is easy to write down recurrence relations for all j_{n+1} and $\overline{j_{n+1}}$ in terms of appropriate i_n and $\overline{i_n}$. All these recurrence relations are obviously linear, so one can employ a well studied theory of systems of linear recurrence relations to solve for all j_n and $\overline{j_n}$.

Solving a system like that basically amounts to finding eigenvalues of the matrix of this system, usually called the *transition matrix*. (Note that all entries of this matrix are nonnegative.) In fact, since we are only interested in the *growth* of $\sum_n j_n + \overline{j_n}$, we only need the maximum real positive eigenvalue (the Perron–Frobenius eigenvalue) of the transition matrix; this will determine the growth type of the tree $\mathrm{WT}(u)$.

Of course, a system like that is, in general, too big; it has $2r$ equations. In most practical situations, however, the set of vertices of the Whitehead graph $\mathrm{Wh}(u)$ can be split into a union of a few (large) sets, and then one can write recurrence relations (still linear) for the numbers of elements in these sets, thus getting a reasonable number of equations.

Finally, we mention that some sets of elements of F_r can be interpreted as Markov processes whose transition matrices arise in a way similar to what we described above. It is conceivable that sets like that are precisely *graphic sets* in the sense of [63].

Proof of Theorem 4.2.1. Let $u \in F_r$, and let $\overline{\mathrm{Wh}(u)}$ be the underlying simple graph of the Whitehead graph $\mathrm{Wh}(u)$ (in particular, $\overline{\mathrm{Wh}(u)}$ has no multiple edges).

There are two principal cases to consider:

Case 1. There is a vertex of degree 1 in $\overline{\mathrm{Wh}(u)}$.

Case 2. The degree of any vertex of the graph $\overline{\mathrm{Wh}(u)}$ is ≥ 2.

In Case 1, suppose that, say, the vertex of $\overline{\mathrm{Wh}(u)}$ corresponding to the generator x_1 has degree 1. That means u has the form $u =$

$u(x_1x_j, x_2, \ldots, x_r)$ for some j. Then the vertex corresponding to x_j^{-1} may have any degree $\leq 2r-1$, whereas other vertices have degrees $\leq 2r-2$.

Thus, the greatest possible number of edges in the graph $\overline{\mathrm{Wh}(u)}$ occurs if $\overline{\mathrm{Wh}(u)}$ has one vertex of degree 1, one vertex of degree $2r-1$, and $2r-2$ vertices of degree $2r-2$. To produce the corresponding transition matrix, we let a_n be the number of vertices labeled x_1 in the nth level of the Whitehead tree $\mathrm{WT}(u)$, b_n the number of vertices labeled x_j^{-1}, c_n the number of vertices labeled x_j, and r_n the number of vertices labeled by other letters. Then we have the following system of linear recurrence relations:

$$\begin{cases} a_{n+1} = b_n + c_n + r_n \\ b_{n+1} = b_n + r_n \\ c_{n+1} = a_n + c_n + r_n \\ r_{n+1} = (b_n + c_n) \cdot (2r-3) + r_n \cdot (2r-4) \end{cases} \tag{4.2}$$

We note that the actual value of r_{n+1} is smaller than $(b_n+c_n)\cdot(2r-3)+r_n \cdot (2r-4)$ because, say, some vertices labeled x_j may be connected to vertices labeled x_j, and not to vertices labeled by "other" letters. However, since we are looking for an upper bound, we are allowed to replace the actual value of r_{n+1} by a greater one.

The transition matrix of this system is

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 2r-3 & 2r-3 & 2r-4 \end{pmatrix}.$$

The characteristic polynomial of this matrix is

$$\lambda^4 - (2r-2)\lambda^3 + (2r-2)\lambda - 1 = (\lambda^2-1)(\lambda^2-(2r-2)\lambda+1),$$

and the Perron–Frobenius eigenvalue is

$$\lambda_{\max} = r - 1 + \sqrt{(r-1)^2-1}.$$

Thus, the number of elements of length n in Case 1 is $O((r-1+\sqrt{(r-1)^2-1})^n)$.

In Case 2, we start with a simple

Lemma 4.2.3. *Suppose the degree of any vertex of a simple graph Γ with $2r$ vertices is ≥ 2. If Γ has either at least two vertices of degree $\geq 2r-2$ or at least one vertex of degree $2r-1$, then any two vertices of Γ can be included in a simple circuit.*

Proof. Let v_1 and v_2 be two vertices of degree $\geq 2r-2$. If they are not adjacent, then they both must be adjacent to all other vertices of the graph Γ. Then, given any two vertices w_1 and w_2 of Γ, we can include them in the simple circuit $w_1 \to v_2 \to w_2 \to v_1 \to w_1$.

If v_1 and v_2 are adjacent, then there might be a vertex w which is not adjacent to either v_1 or v_2 (or both). Suppose w_1 and w_2 are two vertices of Γ. If they both are different from w, then they obviously can be included in a simple circuit. Now suppose, say, $w_1 = w$. Since the degree of any vertex of Γ is ≥ 2, w must be adjacent to a vertex $w_3 \neq w_2$. Then we get a simple circuit $w \to w_3 \to v_2 \to w_2 \to v_1 \to w$.

The case where Γ has a vertex of degree $2r-1$ is similar. ■

From Lemma 4.2.3, we see that if $u \in F_r$ is a primitive element, then at most one vertex of the graph $\overline{\mathrm{Wh}(u)}$ can have degree $\geq 2r-2$, and there are no vertices of degree $2r-1$. If there are no vertices of degree $2r-2$, then the number of elements of length n with the graph $\overline{\mathrm{Wh}(u)}$ like that is obviously bounded by $(2r-3)^n$, so there is nothing to prove.

Thus, the greatest possible number of edges in $\overline{\mathrm{Wh}(u)}$ occurs if $\overline{\mathrm{Wh}(u)}$ has one vertex of degree $2r-2$, and $2r-1$ vertices of degree $2r-3$. We note in passing that, in fact, this cannot happen because, if all vertices of $\overline{\mathrm{Wh}(u)}$ have degrees $\geq 2r-3$, then, since $2r-3 \geq \frac{2r}{2}$, $\overline{\mathrm{Wh}(u)}$ must be Hamiltonian by a classical result of Ore (see, e.g., [402, Theorem 7.1, Corollary 7.2]). A Hamiltonian graph cannot have a cut vertex. However, since we are looking for an upper bound, this is legitimate.

Let now the vertex of degree $2r-2$ have label x_1. It is clear that, for any element u whose graph $\overline{\mathrm{Wh}(u)}$ has properties mentioned above, at every level of the Whitehead tree $\mathrm{WT}(u)$ one has at least $2r-4$ times as many vertices labeled x_i, $i \neq 1$, as one does vertices labeled x_1. We therefore have the following inequalities for the numbers r_n of vertices at level n:

$$r_{n+1} \leq \frac{1}{2r-3} \cdot r_n \cdot (2r-2) + \frac{2r-4}{2r-3} \cdot r_n \cdot (2r-3) = r_n \cdot \left(2r-3+\frac{1}{2r-3}\right).$$

Thus, $r_n \leq c \cdot (2r-3+\frac{1}{2r-3})^n$ for some constant c in this case. Since $2r-3+\frac{1}{2r-3} < r-1+\sqrt{(r-1)^2-1}$, this completes the proof of the theorem. ■

For the group F_2, the number of *cyclically reduced* primitive elements of length $m \geq 1$ can be computed precisely; this number happens to have a rather slow growth (as a function of m). If, however, we drop the condition of being cyclically reduced, the situation changes, and the growth becomes exponential.

Proposition 4.2.4 ([286]). *The number of primitive elements of length m in the group F_2 (and therefore, in any group F_r, $r \geq 2$) is:*

(a) *bigger than $\frac{8}{3\sqrt{3}} \cdot (\sqrt{3})^m$ if m is odd;*

(b) *bigger than $\frac{4}{3} \cdot (\sqrt{3})^m$ if m is even;*

(c) *The number of* cyclically reduced *primitive elements of length $m \geq 1$ in the group F_2 is $4m \cdot \Phi(m)$, where $\Phi(m)$ is the Euler function of m*

(*i.e., the number of positive integers* $< m$ *relatively prime to* m). (*Clearly,* $\Phi(m) < m$.)

Informally speaking, "most" primitive elements in F_2 are conjugates of primitive elements of smaller length. Rivin [315] observed that the number $P(2,m)$ of all primitive elements of length m in F_2 actually grows like $(\sqrt{3})^m$; i.e., the lower bounds given in Proposition 4.2.4 are rather tight in the case of F_2.

Proof of Proposition 4.2.4 Let x and y be generators of F_2.

(a) Suppose m is odd. Then any conjugate of $x^{\pm 1}$, as well as of $y^{\pm 1}$, by an element of length $k = (m-1)/2$, is a primitive element of length m (assuming there are no cancellations in the middle). The number of elements like that in the group F_2 is $2 \cdot 3^{k-1}$, whence the result.

(b) If m is even, then counting conjugates of $x^{\pm 1}y$ and $xy^{\pm 1}$ by elements of length $(m-2)/2$ yields the result.

(c) The result of this part will follow from a well-known fact about primitive elements of F_2 (see [71] or [296]): for any pair $\{k,l\}$ of integers with $(k,l) = 1$, there is exactly one cyclically reduced primitive element of F_2 whose exponent sum on x is k and the exponent sum on y is l.

Thus, the number of cyclically reduced primitive elements of F_2 of length m is 8 times the number of pairs $\{k,l\}$ of *positive* integers with $(k,l) = 1$, $k < l$, $k + l = m$. The latter number is obviously equal to $\frac{1}{2}\Phi(m)$, where $\Phi(m)$ is the number of positive integers $< m$ relatively prime to m. ■

4.2.2 Complexity of Whitehead's algorithm

In this section, we study the complexity of Whitehead's algorithm that determines whether or not a given element of a free group of finite rank is an automorphic image of another given element.

It is known that the first part of this algorithm (reducing a given free word to a free word of minimum possible length by "elementary" Whitehead automorphisms) is pretty fast (of quadratic time with respect to the length of the word). On the other hand, the second part of the algorithm (applied to two words of the same minimum length) was always considered very slow. In fact, the procedure outlined in the original paper by Whitehead [400] suggested this part of the algorithm to be of superexponential time with respect to the length of the words. Indeed, given a word u, the procedure calls for constructing a graph whose vertices correspond to all words of length $|u|$. This means that the number of vertices is an exponential function of $|u|$. After that, for every vertex of the graph, one constructs edges incident to this vertex as follows: an edge connects this particular vertex to another vertex if and only if there is an elementary Whitehead automorphism that takes one of the corresponding words to the other. Finally, to find out if there is an automorphism that takes the word u to another given word v of the same length, one has to check all the paths in

the graph that start at the vertex that corresponds to u and see if some of them lead to the vertex that corresponds to u. The number of paths in a graph is, in general, an exponential function of the number of vertices. Therefore this algorithm is, in general, of superexponential complexity with respect to the length of the word u.

It is possible, however, to skip some steps in this algorithm and get the following:

Proposition 4.2.5. *Let N be the number of automorphic images of $u \in F_n$ that have the same length as u does. Then, given an element v of length $|u|$, one can decide in quadratic time with respect to N whether or not v is an automorphic image of u.*

Proof. We are going to use the *backtracking* method, which is a well-known procedure in graph theory for searching a tree.

Starting with the vertex that corresponds to $u = u_0$, we are building a tree as follows. (We use the same notation for words and corresponding vertices when there is no ambiguity.)

(1) Apply an arbitrary elementary Whitehead automorphism to u_0; if a new word u_1 of the same length is obtained, plot the corresponding vertex and connect it to u_0. If not, then apply another elementary Whitehead automorphism until you get a new word u_1 of the same length. (Note that the total number of those automorphisms $C = C(n)$ is finite and depends on the rank n of the group F_n only.)

(2) Continue the same process. That is, suppose we have obtained a word u_i, $i > 0$, at the previous step. This time "a new word" would mean a word different from all the words obtained at previous steps.

If none of the elementary Whitehead automorphisms produces a new word, then do "backtracking" (i.e., return to the word obtained at the immediately preceding step, and repeat the same process).

In the end (i.e., when no new word can be obtained from any of the "old" words), we shall obviously have a *spanning tree* of the graph described before the statement of Proposition 4.2.5. It will therefore have N vertices and $N - 1$ edges. Furthermore, in the course of constructing this tree, we did not visit any of the vertices more than N times because to obtain any new vertex we had to visit other vertices no more than once.

Thus, the time we need to construct this tree is no more than $C \cdot N^2$, where C is the constant mentioned above. Once the tree is constructed, it will take just N more steps to find out if the vertex corresponding to the word v is among the vertices; or, we can perform the check every time we get a new vertex because once we get v we can stop. ■

Furthermore, in the case where the free group has rank 2, we have

Theorem 4.2.6 ([286]). *Let $u \in F_2$ be a word whose length is irreducible by any automorphism of F_2 (in particular, u is cyclically reduced). Then*

the number of automorphic images of u that have the same length as u does is bounded by a polynomial function of $|u|$.

In fact, experimental data suggest that the number in the statement of Theorem 4.2.6 has the (exact!) bound of $8m^2 - 40m$ for $m \geq 9$, where $m = |u|$ (and, therefore, $8m - 40$ if one counts *cyclic* words). Recently, D. Lee [207] was able to prove this.

Theorem 4.2.6 has the following corollary:

Corollary 4.2.7. *In the group F_2, Whitehead's algorithm terminates in polynomial time with respect to the maximum length of the two words in question.*

By the aforementioned result of D. Lee, Whitehead's algorithm in F_2 actually terminates in quadratic time with respect to the maximum length of the two words.

We also mention here an interesting "statistical" result from [172] even though it is outside of the scope of this book: for "most" inputs (in a precise sense), Whitehead's algorithm in F_n, $n \geq 2$, terminates in linear time with respect to the maximum length of the inputs.

We do not know whether or not Theorem 4.2.6 and, therefore, Corollary 4.2.7 hold for free groups of bigger ranks. However, experimental data kindly provided by C. Sims allowed Myasnikov and Shpilrain [286] to make the following conjecture:

Conjecture 4.2.8 ([286]). In the free group F_n, the cardinality of $A(u)$ is bounded by a polynomial of degree $2n - 2$ in $|u|$, provided the length of u is irreducible by any automorphism of F_n.

A most amazing thing is that, according to the experimental data mentioned above, the *maximum* cardinality of $A(u)$ that can actually occur under the irreducibility assumption in Conjecture 4.2.8 appears to be *precisely* a polynomial of degree $2n - 2$ in $m = |u|$ for sufficiently large m. For $n = 2$, this polynomial, as we have already mentioned, is $8m^2 - 40m$ if $m \geq 9$. For $n = 3$, the polynomial is $48m^4 - 480m^3 + 1104m^2 - 672m$ if $m \geq 11$. A particular element $u \in F_3$ of length m whose orbit $A(u)$ has the cardinality given by the latter polynomial is, according to the same experimental data, $u = x_1^k x_2 x_1 x_2^{-1} x_1 x_2^2 x_3^2$, where $k = m - 8$.

D. Lee [207] was able to prove, under some mild restrictions on u, that the cardinality of $A(u)$ is bounded by a polynomial of degree $n(3n - 5)/2$ in $|u|$.

We also note that, in the case where the free group has rank 2 (but not in the general case), the condition on $|u|$ to be irreducible by any automorphism can be relaxed to u just being cyclically reduced.

Proof of Theorem 4.2.6. Throughout the proof, we shall call "length-preserving" those automorphisms of F_2 that are permutations on the set $\{x, x^{-1}, y, y^{-1}\}$. There are eight of them, so whenever we count the number

of automorphic images of a particular element "up to a length-preserving automorphism", it means the upper bound for such a number should be multiplied by 8.

Let $M = |u|$. Let k be the sum of exponents on x in the word u, and let l be the sum of exponents on y. Upon applying a length-preserving automorphism if necessary, we may assume that $k, l \geq 0$. First, we are going to establish the result of Theorem 4.2.6 for $u \notin [F_2, F_2]$, so we assume that k, l are not both 0. In this case, the result will follow from the following observations.

(1) For a word of length M, there are $\sum_{i=0}^{M}(i+1) = \frac{1}{2}(M+1)(M+2)$ possible pairs (k, l) with $k, l \geq 0$; $k + l \leq M$.

(2) It is well-known (see, e.g., [231]) that the group $\mathrm{Aut}(F_2)$ is generated by inner automorphisms, by three length-preserving automorphisms $\pi\colon x \to y,\ y \to x$; $\sigma_x\colon x \to x^{-1},\ y \to y$; $\sigma_y\colon x \to x,\ y \to y^{-1}$, and by the following two: $\alpha\colon x \to xy,\ y \to y$, and $\beta\colon x \to x,\ y \to yx$. The subgroup H of $\mathrm{Aut}(F_2)$ generated by α and β can be mapped onto $\mathrm{SL}_2(\mathbb{Z})$. Under this epimorphism, α and β correspond to the matrices $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, respectively. The kernel of this epimorphism is generated (as a normal subgroup) by the inner automorphism induced by the element $[x, y]$; in particular, every automorphism in the kernel is inner.

Furthermore, relations between generators of $\mathrm{Aut}(F_k)$ given in [231, Section 3.5, Theorem N1] show that, in any product of automorphisms $\alpha^{\pm 1}$, $\beta^{\pm 1}$, π, σ_x, and σ_y, automorphisms $\alpha^{\pm 1}$ and $\beta^{\pm 1}$ can be collected on the right. This, together with the fact that the subgroup of inner automorphisms of F_2 is normal in $\mathrm{Aut}(F_2)$, implies that applying an automorphism of F_2 amounts to first applying an automorphism from the subgroup H generated by α and β, then a length-preserving automorphism, and, finally, an inner automorphism.

Therefore, to bound the number of cyclically reduced automorphic images of u with the same nonzero vector (k, l) of exponent sums, it is sufficient to bound the number of matrices from $\mathrm{SL}_2(\mathbb{Z})$ that fix the vector (k, l) acted upon by right multiplication and then multiply this number by M (the number of cyclic permutations of a word of length M). Furthermore, up to a length-preserving automorphism, every automorphism from the group H corresponds to a matrix from $\mathrm{SL}_2(\mathbb{Z})$ whose elements in the first row are of different signs, say, the element in the upper left corner is nonnegative and the element in the upper right corner is nonpositive. (Elements in the first row correspond to the image of x.)

(3) Thus, what is left to do now is to count the number of matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose elements in the first row are of different signs that fix a given nonzero vector (k, l) with $k, l \geq 0$. The computation here is straightforward. Let $A = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$ be a matrix from $\mathrm{SL}_2(\mathbb{Z})$ with $a_{11} \geq 0$, $a_{12} \leq 0$, which

fixes a vector (k, l). Then we have the following system of equations in a_{ij}:

$$\begin{aligned} k \cdot a_{11} + l \cdot a_{21} &= k, \\ k \cdot a_{12} + l \cdot a_{22} &= l, \\ a_{11}a_{22} - a_{12}a_{21} &= 1. \end{aligned}$$

Suppose first that both $k, l \neq 0$. Then, from the first equation, we get $a_{21} = \frac{k}{l} - \frac{k}{l} \cdot a_{11}$, and from the second equation $a_{22} = 1 - \frac{k}{l} \cdot a_{12}$. Plug this into the third equation and simplify: $l \cdot a_{11} - k \cdot a_{12} = l$. Since $k, l > 0$, $a_{11} \geq 0$, $a_{12} \leq 0$, this gives either $a_{12} = 0$, $a_{11} = 1$, or $a_{11} = 0$, $a_{12} = -\frac{l}{k}$. In the former case, we get $a_{22} = 1$, $a_{21} = 0$. In the latter case, $a_{21} = \frac{k}{l}$, $a_{11} = 0$, $a_{22} = 2$.

Now suppose, say, $k = 0$. Then $a_{21} = 0$, $a_{22} = 1$, $a_{11} = 1$, whereas a_{12} can be arbitrary. However, we can show that, should the automorphism corresponding to the matrix A preserve the length of u, the absolute value of a_{12} cannot be greater than $2|u|$. Indeed, let $K = a_{12}$; then the automorphism corresponding to the matrix A is α^K (i.e., it takes x to xy^K, y to y). Suppose $K > 2|u|$; we may assume that u has at least one occurrence of x. Then $\alpha^K(u)$ has a subword xy^K (before cancellation). Since we have assumed that $\alpha^K(u)$ has the same length as u does, more than half of y^K should cancel out. This implies that, in the word u itself, there is a subword y^{-N} with $N \geq \frac{K+1}{2}$. This is a contradiction since $K > 2|u|$.

Thus, in any of the cases considered, we have no more than $2|u|$ different matrices from $\mathrm{SL}_2(\mathbb{Z})$ that fix a given nonzero vector (k, l).

Summarizing the observations (1), (2), and (3), we see that the number of cyclically reduced automorphic images of u of length $M = |u|$ is no more than $c \cdot M^4$ for some constant c independent of u. This completes the proof in the case where $u \notin [F_2, F_2]$.

Now let $u \in [F_2, F_2]$. In this case, we are going to use induction on the length of u. To make the induction work, we are going to prove the following somewhat stronger claim.

Proposition 4.2.9. *Let $u \in [F_2, F_2]$ be cyclically reduced. For any positive integer K, the number of elements $v \in F_2$ such that $v = \varphi(u)$ for some $\varphi \in \mathrm{Aut}(F_2)$ and $|v| = |u| + K$ is less than $c \cdot 3^K \cdot (|u| + K)^4$ for some constant c independent of u and K.*

Proof. The basis of induction $u = [x, y]$ is almost obvious. This element is fixed by any automorphism from H (recall that H is the subgroup of $\mathrm{Aut}(F_2)$ generated by two automorphisms, $\alpha\colon x \to xy$, $y \to y$, and $\beta\colon x \to x$, $y \to yx$), and therefore, to count the number of elements $v \in F_2$ such that $v = \varphi(u)$ for some $\varphi \in \mathrm{Aut}(F_2)$ and $|v| = |u| + K$, we just have to count (up to a length-preserving automorphism) the number of conjugates of u of length up to $|u| + K$. This latter number is no bigger than the number of different elements of length $[K/2]$ in the group F_2 (i.e., it equals $3^{[K/2]}$).

For the induction step, we first assume that u has a subword of the form $[x^{\pm 1}, y^{\pm 1}]$. Then, upon applying a length-preserving automorphism if necessary, we may assume that u has a subword $[x, y]$. Then a cyclic permutation of u has the form $[x, y]w$, with no cancellation between $[x, y]$ and w. Thus, by the remarks in the beginning of the proof of Theorem 4.2.6, we may assume that $u = [x, y]w$. Let φ be an arbitrary automorphism from H. Recall that every automorphism in H fixes $[x, y]$.

Assume first that w is cyclically reduced. We have two possibilities:

(1) $[x, y]$ is entirely cancelled out by $\varphi(w)$. Then, since $\varphi(u) = [x, y]\varphi(w)$, we see that, if $|\varphi(u)| = |u| + K$, we must have $|\varphi(w)| = |w| + K + 4$. By the inductive assumption, the number of automorphic images of w with this property is no more than $c \cdot 3^{K+4} \cdot |w + K + 4|^4$ for some constant c independent of w and K. A similar result for u now follows.

(2) Only part of $[x, y]$ cancels out (this includes the case where nothing cancels out). Then, since $\varphi(u) = [x, y]\varphi(w)$ and since an element of the commutator subgroup must have an even length, we see that, if $|\varphi(u)| = |u| + K$, then either $|\varphi(w)| = |w| + K + 2$ or $|\varphi(w)| = |w| + K$. By the inductive assumption, the number of automorphic images of w with this property is no more than $c \cdot 3^{K+2} \cdot |w+K+2|^4$ (respectively, $c \cdot 3^K \cdot |w+K|^4$) for some constant c independent of w and K. A similar result for u now follows.

If w is not cyclically reduced (i.e., if $u = [x, y]gw'g^{-1}$), then we consider a cyclic permutation of u: $u' = g^{-1}[x, y]gw' = [x^{g^{-1}}, y^{g^{-1}}]w'$, where we can assume w' to be cyclically reduced. Now we apply essentially the same argument to u' as we have just applied to u, upon replacing the subgroup H of automorphisms by the left coset $i_g H$, where i_g is the inner automorphism induced by the element g. (Applying an automorphism from $i_g H$ is equivalent to first applying conjugation by g and then applying an automorphism from H.)

Since the group of inner automorphisms is normal in $\mathrm{Aut}(F_2)$, observation (2) in the beginning of the proof of Theorem 4.2.6 remains valid upon replacing H by $i_g H$. That is, every automorphism from $\mathrm{Aut}(F_2)$ is a product of an automorphism from the coset $i_g H$ and an inner automorphism. Since every automorphism from $i_g H$ fixes the element $[x^{g^{-1}}, y^{g^{-1}}]$, the same argument as above completes the proof in this case.

Suppose now that u does not have a subword of the form $[x^{\pm 1}, y^{\pm 1}]$ but does have a subword of the form $x^{\pm 1}y^{\pm 1}x^{\mp 1}$. Then, upon applying a length-preserving automorphism if necessary, we may assume that u has a subword xyx^{-1}. Thus, a cyclic permutation of u has the form $xyx^{-1}w$, with no cancellation. Then we can write u as $u = [x, y]yw$. Note that the word yw has smaller length than u does, and we can assume that yw is cyclically reduced, for if it was not, w would end with y^{-1}, and then a cyclic permutation of u would be of the form $y^{-1}xyx^{-1}w' = [y^{-1}, x]w'$, and therefore this case would be reduced to the previous one.

Thus, we can apply the inductive assumption to this word w, and the same argument as above will work in this case as well.

Finally, suppose that u does not have a subword of the form $x^{\pm 1}y^{\pm 1}x^{\mp 1}$. Then u must have a subword of the form $x^{\pm 1}y^k x^{\mp 1}$ for some $k \neq 0, \pm 1$. We can assume, upon applying a length-preserving automorphism and a cyclic permutation if necessary, that $u = xy^k x^{-1} w$, $k > 1$. Then we can write $u = [x, y]yxy^{k-1}x^{-1}w$. Now the word $yxy^{k-1}x^{-1}w$ has the same length as u does, but it has the subword $xy^{k-1}x^{-1}$. Also, we can assume that yw is cyclically reduced, for if it was not, w would end with y^{-1}, and then a cyclic permutation of u would be of the form $y^{-1}xy^k x^{-1}w'$ (i.e., it would begin with $y^{-1}xy$), and therefore this case would be reduced to one of those previously considered. An obvious inductive argument now completes the proof. ■

4.3 Endomorphisms that Preserve Automorphic Orbits

In this section, we are going to give a solution to Problem 4.0.2. Our exposition here follows [206].

As usual, let F_n be the free group of a finite rank n on the set $\mathfrak{X} = \{x_1, \dots, x_n\}$ of free generators.

Theorem 4.3.1. *Suppose φ is an endomorphism of F_n such that $\varphi\,\mathrm{Orb}_{\mathrm{Aut}\,F_n}(W) \subseteq \mathrm{Orb}_{\mathrm{Aut}\,F_n}(W)$ for some $W \in F_n$, $W \neq 1$. Then φ is an automorphism of F_n.*

Recall that a sequence $\mathfrak{U} = (u_1, u_2, \dots)$ of words of F_n is called *N-reduced* (Nielsen reduced) if every $u_i \in \mathfrak{U}$ is reduced and, for any triple v_1, v_2, v_3 of the form $u_i^{\pm 1}$, where $u_i \in \mathfrak{U}$, the following three conditions hold (see Section 1.1):

- (N1) $v_1 \neq 1$;
- (N2) $v_1 v_2 \neq 1$ implies $|v_1 v_2| \geq |v_1|, |v_2|$;
- (N3) $v_1 v_2 \neq 1$ and $v_2 v_3 \neq 1$ implies $|v_1 v_2 v_3| > |v_1| - |v_2| + |v_3|$.

It is well-known that if $\mathfrak{U} = (u_1, u_2, \dots)$ is N-reduced, then the subgroup $\langle \mathfrak{U} \rangle$ of F_n generated by $\mathfrak{U}$ is free with the basis $\mathfrak{U}$. Also, every finite sequence of reduced words of F_n can be carried by Nielsen transformations (see Section 1.1) to some N-reduced sequence.

Recall also that a *Whitehead automorphism* ω of F_n is an automorphism of one of the following two types (see Section 1.2):

- (W1) ω permutes elements in $\mathfrak{X}^{\pm 1}$;

- (W2) ω is defined by a set $\mathcal{S} \subset \mathfrak{X}^{\pm 1}$ and a letter $a \in \mathfrak{X}^{\pm 1}$ with $a \in \mathcal{S}$ and $a^{-1} \notin \mathcal{S}$ in such a way that if $x \in \mathfrak{X}^{\pm 1}$ then (a) $\omega(x) = x$ provided $x = a^{\pm 1}$; (b) $\omega(x) = xa$ provided $x \neq a$, $x \in \mathcal{S}$, and $x^{-1} \notin \mathcal{S}$; (c) $\omega(x) = a^{-1}xa$ provided both $x, x^{-1} \in \mathcal{S}$; (d) $\omega(x) = x$ provided both $x, x^{-1} \notin \mathcal{S}$.

If ω is of the type (W2), then we write $\omega = \omega(\mathcal{S}, a)$. We also need the *standard Whitehead graph* $\Phi(Y)$, which is constructed as follows (see, e.g., [227]). Take $\mathfrak{X}^{\pm 1}$ as the vertex set, and connect two vertices $a, b \in \mathfrak{X}^{\pm 1}$ by a nonoriented edge if there is a subword ab^{-1} or ba^{-1} of (noncyclic) Y. We let $C(a, Y)$ denote the connected component of $\Phi(Y)$ containing a vertex $a \in \Phi(Y)$.

As usual, by writing $X \equiv Y$ we mean the graphical equality (letter-by-letter) of words $X, Y \in F_n$ (whereas $X = Y$ means the equality of X, Y in F_n). By $\bar{X}$ we denote a reduced word equal in F_n to X and by $|X|$ the length of a word X of F_n with respect to the basis $\mathfrak{X}$.

Proof of Theorem 4.3.1. Without loss of generality, we may assume that W has the minimum length over all words in $\mathrm{Orb}_{\mathrm{Aut}\, F_n}(W)$. Then the *rank of* W is defined to be the number of elements of $\mathfrak{X}$ occurring in W. We consider two cases corresponding to whether W has rank 1 or not.

Case 1. W has rank 1.

If W is a primitive element of F_n, then there is nothing to prove due to the result of [205]. Also, if W is a proper power of a primitive element of F_n, then the assertion follows immediately by combining the result of [205] and the fact that extraction of roots in a free group is unique.

Case 2. W has rank r with $1 < r \leq n$.

Upon permuting elements of $\mathfrak{X}$, we can assume that only the elements $x_1, x_2, \ldots, x_r$ of $\mathfrak{X}$ occur in W. We may further assume, by interchanging x_i and x_i^{-1} and then permuting the elements $x_1, x_2, \ldots, x_r$ if necessary, that

$$x_1 \text{ has positive exponent sum in } W \quad \text{unless every } x_i \text{ has zero exponent sum in } W. \tag{4.3}$$

Now let u be a primitive element of F_n. Due to the result of [205], it is enough to prove that $\varphi(u)$ is also primitive. By definition of a primitive element, there is $\alpha \in \mathrm{Aut}\, F_n$ such that $\alpha(x_1) = u$. Note that $\varphi \circ \alpha$ has the same property as φ does; that is, $(\varphi \circ \alpha)\, \mathrm{Orb}_{\mathrm{Aut}\, F_n}(W) \subseteq \mathrm{Orb}_{\mathrm{Aut}\, F_n}(W)$. Hence, upon replacing $\varphi \circ \alpha$ by φ, it suffices to prove that $\varphi(x_1)$ is primitive.

Let F_r, F_{n+1} be the free groups on the sets $\mathfrak{X}_r = \{x_1, x_2, \ldots, x_r\}$, $\mathfrak{X}_{n+1} = \{x_1, x_2, \ldots, x_{n+1}\}$, respectively. Obviously, F_r is a free factor of F_n of rank r. Now we want to prove:

Claim 1. *The restriction $\varphi|_{F_r}$ of φ to F_r is a monomorphism.*

Proof. Suppose, by way of contradiction, that $\varphi|_{F_r}$ is not a monomorphism. Consider the finite sequence $(\varphi(x_1), \varphi(x_2), \ldots, \varphi(x_r))$. This sequence can be brought to an N-reduced one by Nielsen transformations. This fact implies the existence of $\delta \in \operatorname{Aut} F_r$ such that $(\varphi \circ \delta)(x_1) = \cdots = (\varphi \circ \delta)(x_k) = 1$ and that the sequence $((\varphi \circ \delta)(x_{k+1}), \ldots, (\varphi \circ \delta)(x_r))$ is N-reduced. (Note that $k \geq 1$ since $\varphi|_{F_r}$ is not a monomorphism.) For the sake of simplicity of notation, we put

$$U_i = (\varphi \circ \delta)(x_i) \quad \text{for} \quad i = k+1, \ldots, r.$$

Define $\varepsilon \in \operatorname{Aut} F_r$ as

$$\varepsilon(x_1) = x_1[x_{k+1}^{\ell} x_{k+2}^{\ell} \ldots x_{r-1}^{\ell} x_r^{\ell} x_{r-1}^{\ell} \ldots x_{k+2}^{\ell} x_{k+1}^{\ell}] \quad \text{and}$$
$$\varepsilon(x_i) = x_i \quad \text{for} \quad i = 2, \ldots, r,$$

where ℓ is a sufficiently large integer. Now consider $(\varphi \circ \delta \circ \varepsilon)(W)$. Since $(\delta \circ \varepsilon)(W)$ belongs to $\operatorname{Orb}_{\operatorname{Aut} F_n}(W)$, $(\varphi \circ \delta \circ \varepsilon)(W)$ is in $\operatorname{Orb}_{\operatorname{Aut} F_n}(W)$ by the hypothesis of the theorem. If $k = r-1$, then by (4.3) we have either $(\varphi \circ \delta \circ \varepsilon)(W) = 1$ or $(\varphi \circ \delta \circ \varepsilon)(W) = U_r^{\ell'}$ with ℓ' being sufficiently large (so $\ell' > |W|$). The former case contradicts $(\varphi \circ \delta \circ \varepsilon)(W) \in \operatorname{Orb}_{\operatorname{Aut} F_n}(W)$. So does the latter case because, for simple words u and v in F_n (i.e., u and v are nonempty, cyclically reduced, and not proper powers), the equality $u^m = v^{m'}$ with $m, m' > 0$ implies that $u = v$ and $m = m'$. Hence, k has to be less than $r-1$.

Let $\beta\colon F_n \to F_{n+1}$ be a homomorphism given by

$$\beta(x_1) = x_{n+1} \quad \text{and} \quad \beta(x_i) = (\varphi \circ \delta)(x_i) \quad \text{for} \quad i = 2, \ldots, n.$$

Since $(\varphi \circ \delta)(W) \in \operatorname{Orb}_{\operatorname{Aut} F_n}(W)$ by the hypothesis of the theorem, clearly $(\varphi \circ \delta)(W) \neq 1$. This implies that we may assume, by permuting the elements $x_1, x_2, \ldots, x_r$ if necessary, that

$$\text{at least one } x_{n+1} \text{ remains uncancelled in } \overline{\beta(W)}. \tag{4.4}$$

It follows from $(\varphi \circ \delta)(x_1) = \cdots = (\varphi \circ \delta)(x_k) = 1$ that

$$(\varphi \circ \delta \circ \varepsilon)(W) = Z_0 K^{t_1} Z_1 K^{t_2} Z_2 \ldots K^{t_p} Z_p,$$

where $K = U_{k+1}^{\ell} U_{k+2}^{\ell} \ldots U_{r-1}^{\ell} U_r^{\ell} U_{r-1}^{\ell} \ldots U_{k+2}^{\ell} U_{k+1}^{\ell}$, $t_i \in \mathbb{Z} \setminus \{0\}$, $1 \leq p < |W|$, Z_i is a product of elements of $\{U_{k+1}^{\pm 1}, \ldots, U_r^{\pm 1}\}$, and only Z_0 and Z_p may be trivial. Since $(\varphi \circ \delta \circ \varepsilon)(W) \in \operatorname{Orb}_{\operatorname{Aut} F_n}(W)$, there is $\zeta \in \operatorname{Aut} F_n$ such that $(\zeta \circ \varphi \circ \delta \circ \varepsilon)(W) = W$. For such $\zeta \in \operatorname{Aut} F_n$, we have

$$W = (\zeta \circ \varphi \circ \delta \circ \varepsilon)(W) = \zeta(Z_0)\, \zeta(K)^{t_1} \zeta(Z_1)\, \zeta(K)^{t_2} \zeta(Z_2) \ldots \zeta(K)^{t_p} \zeta(Z_p). \tag{4.5}$$

Let us write

$$\overline{\zeta(U_i)} \equiv Y_i X_i^{s_i} Y_i^{-1} \quad \text{for} \quad i = k+1, \ldots, r,$$

where $s_i \in \mathbb{Z}_+$ and X_i is a simple word in F_n.

Suppose that the product on the right-hand side of (4.5) involves a cancellation between $X_i^{\pm s_i \ell}$ and $X_j^{\pm s_j \ell}$ such that a part of $X_i^{\pm s_i \ell}$ of length greater than $|X_i|+|X_j|$ cancels with a part of $X_j^{\pm s_j \ell}$ of length greater than $|X_i|+|X_j|$. We first assume that such a cancellation occurs in a subproduct of the form

$$X_i^{-s_i \ell} Y_i^{-1} \zeta(Z)\, Y_j\, X_j^{s_j \ell},$$

where Z is a product of elements of $\{U_{k+1}^{\pm 1}, \dots, U_r^{\pm 1}\}$. It is not hard to prove that if u, v are simple words in F_n and w is a subword of both u^m and $v^{m'}$ with $m, m' > 0$ such that $|w| \geq |u| + |v|$, then u is a cyclic permutation of v. This implies that X_i is a cyclic permutation of X_j. So, if the part of $X_j^{s_j \ell}$ that cancels with a part of $X_i^{-s_i \ell}$ begins with T, where $|T| = |X_j|$, then we can write $X_i = ATA^{-1}$ and $X_j = BTB^{-1}$ for some $A, B \in F_n$. From the fact that no nontrivial cyclic permutation of a simple word u can be u itself, we must have

$$A^{-1} X_i^{-m} Y_i^{-1} \zeta(Z)\, Y_j\, X_j^{m'} B = 1$$

for some $m, m' \in \mathbb{Z}_+ \cup \{0\}$. Thus,

$$1 = A^{-1} X_i^{-m} Y_i^{-1} \zeta(Z)\, Y_j\, X_j^{m'} B = T^{-m} A^{-1} Y_i^{-1} \zeta(Z)\, Y_j\, B\, T^{m'},$$

and hence

$$\zeta(Z) = Y_i\, A\, T^{m-m'} B^{-1} Y_j^{-1}. \tag{4.6}$$

Consider $\zeta(U_i^{-s_j})\, \zeta(Z)\, \zeta(U_j^{s_i})$. We can observe that

$$\begin{aligned}
\zeta(U_i^{-s_j})\, \zeta(Z)\, \zeta(U_j^{s_i}) &= Y_i\, X_i^{-s_i s_j} Y_i^{-1} \zeta(Z)\, Y_j\, X_j^{s_i s_j} Y_j^{-1} \\
&= Y_i\, A\, T^{-s_i s_j} A^{-1} Y_i^{-1} \zeta(Z)\, Y_j\, B\, T^{s_i s_j} B^{-1} Y_j^{-1} \\
&= Y_i\, A\, T^{m-m'} B^{-1} Y_j^{-1} \quad \text{by (4.6)} \\
&= \zeta(Z) \quad \text{again by (4.6)}.
\end{aligned}$$

It then follows from $\zeta \in \operatorname{Aut} F_n$ that

$$U_i^{-s_j}\, Z\, U_j^{s_i} = Z. \tag{4.7}$$

Since Z is a product of elements of $\{U_{k+1}^{\pm 1}, \dots, U_r^{\pm 1}\}$ and the sequence $(U_{k+1}, \dots, U_r)$ is N-reduced, equality (4.7) can hold only when $i = j$ and U_i and Z belong to the same cyclic subgroup of F_n. Here, if Z contained U_j other than $U_i^{\pm 1}$, we would have a contradiction with the fact that the sequence $(U_{k+1}, \dots, U_r)$ is N-reduced. Hence, Z must be either trivial or a power of U_i.

In a similar way, we can prove that only when $i = j$ and Z is either trivial or a power of U_i can there be a cancellation in a subproduct of the form $X_i^{s_i \ell} Y_i^{-1} \zeta(Z)\, Y_j\, X_j^{-s_j \ell}$ such that a part of $X_i^{s_i \ell}$ of length greater than

$|X_i| + |X_j|$ cancels with a part of $X_j^{-s_j\ell}$ of length greater than $|X_i| + |X_j|$. Also, arguing similarly, we can show that such a cancellation cannot occur between $X_i^{s_i\ell}$ and $X_j^{s_j\ell}$ or between $X_i^{-s_i\ell}$ and $X_j^{-s_j\ell}$.

It then follows from (4.4) that after all cancellations in the product on the right-hand side of (4.5) are performed, some $X_i^{\ell'}$, with ℓ' being sufficiently large (so $\ell' > |W|$), must remain uncancelled. This contradiction to equality (4.5) completes the proof of Claim 1. ■

Since $\varphi(W) \in \mathrm{Orb}_{\mathrm{Aut}\, F_n}(W)$, there is $\gamma \in \mathrm{Aut}\, F_n$ such that $(\gamma \circ \varphi)(W) = W$. Hence, upon replacing $\gamma \circ \varphi$ by φ, we may assume that

$$\varphi(W) = W. \tag{4.8}$$

Under this assumption, we are going to prove:

Claim 2. $\varphi(F_r) = F_r$.

Proof. Since $\varphi|_{F_r}$ is a monomorphism by Claim 1, we must have, for such $\delta \in \mathrm{Aut}\, F_r$ as in the proof of Claim 1, that the sequence $((\varphi \circ \delta)(x_1), (\varphi \circ \delta)(x_2), \ldots, (\varphi \circ \delta)(x_r))$ is N-reduced. As above, we write U_i for $(\varphi \circ \delta)(x_i)$, where $i = 1, 2, \ldots, r$.

Clearly the set $\delta(\mathfrak{X}_r) = \{\delta(x_1), \delta(x_2), \ldots, \delta(x_r)\}$ is also a basis of F_r, which yields that W can be expressed in terms of $\delta(x_i)$'s. In this expression, say, W_δ (i.e., W_δ is a word in $\delta(\mathfrak{X}_r)^{\pm 1}$), every $\delta(x_i)$, for $i = 1, 2, \ldots, r$, must occur in W_δ since W has rank r. Furthermore, since W has the minimum length over all words in $\mathrm{Orb}_{\mathrm{Aut}\, F_n}(W)$, the length of W_δ with respect to the basis $\delta(\mathfrak{X}_r)$ must be at least $|W|$.

Consider $\varphi(W_\delta)$. Obviously, $\varphi(W_\delta) = W$ by (4.8) and is a product of elements of $\{U_1^{\pm 1}, U_2^{\pm 1}, \ldots, U_r^{\pm 1}\}$, say,

$$W = \varphi(W_\delta) = U_{q_1}^{\theta_1} U_{q_2}^{\theta_2} \ldots U_{q_m}^{\theta_m}, \tag{4.9}$$

where $q_i \in \{1, 2, \ldots, r\}$, $\theta_i = \pm 1$, and $U_{q_i}^{\theta_i} U_{q_{i+1}}^{\theta_{i+1}} \neq 1$. Then m is equal to the length of W_δ with respect to the basis $\delta(\mathfrak{X}_r)$ and hence $m \geq |W|$. Since the sequence $(U_1, U_2, \ldots, U_r)$ is N-reduced, for every i some part of $U_{q_i}^{\theta_i}$, say, $V_{q_i}^{\theta_i}$, must remain uncancelled in product (4.9) after all cancellations are made; that is,

$$W \equiv V_{q_1}^{\theta_1} V_{q_2}^{\theta_2} \ldots V_{q_m}^{\theta_m}. \tag{4.10}$$

Since $m \geq |W|$, each $|V_{q_i}| = 1$ and hence

$$x_{q_i}^{\theta'} = V_{q_i} = V_{q_j} = x_{q_j}^{\theta'} \quad \text{if and only if } q_i = q_j,$$

where $\theta' = \pm 1$. Replacing, if necessary, $U_{q_i}^{-1}$ and $-\theta_i$ by U_{q_i} and θ_i, respectively, we may assume $\theta' = 1$; that is,

$$x_{q_i} = V_{q_i} = V_{q_j} = x_{q_j} \quad \text{if and only if } q_i = q_j. \tag{4.11}$$

Here, if $U_{q_i} = V_{q_i}$ for every $i = 1, 2, \ldots, m$, then the assertion follows immediately from (4.10) and (4.11). So suppose that there is some i such

that $U_{q_i} \neq V_{q_i}$. Let j be the smallest index such that $U_{q_j}^{\theta_j} \neq V_{q_j}^{\theta_j}$. Then there is no cancellation in the product $U_{q_{j-1}}^{\theta_{j-1}} U_{q_j}^{\theta_j}$, and no more than half of $U_{q_j}^{\theta_j}$ cancels in the product $U_{q_j}^{\theta_j} U_{q_{j+1}}^{\theta_{j+1}}$ because the sequence $(U_1, U_2, \ldots, U_r)$ is N-reduced. Hence we must have

$$U_{q_j}^{\theta_j} = x_{q_j}^{\theta_j} x_s^{\pm 1} \tag{4.12}$$

for some $s \in \{1, 2, \ldots, n\}$.

By (4.9)–(4.12) and the fact that the sequence $(U_1, U_2, \ldots, U_r)$ is N-reduced, there is a Whitehead automorphism $\omega_1 = \omega_1(\mathcal{A}, x_{n+1})$ of F_{n+1} such that $\mathcal{A} \subseteq \{x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_r^{\pm 1}\}$, $x_{q_j}^{\theta_j} \in \mathcal{A}$, $x_{q_j}^{-\theta_j} \notin \mathcal{A}$, and $\omega_1(W) = W$. This implies that the connected component $C(x_{q_j}^{\theta_j}, W)$ of the Whitehead graph $\Phi(W)$ containing a vertex $x_{q_j}^{\theta_j}$ does not contain $x_{q_j}^{-\theta_j}$ and that a Whitehead automorphism ω_2 of F_{n+1} given by $\omega_2 = \omega_2(C(x_{q_j}^{\theta_j}, W), x_{n+1})$ fixes W. The fact $\omega_2(W) = W$ yields $x_{q_1}^{-\theta_1}, x_{q_m}^{\theta_m} \notin C(x_{q_j}^{\theta_j}, W)$. But then, a Whitehead automorphism ω_3 of F_n defined by $\omega_3 = \omega_3(C(x_{q_j}^{\theta_j}, W), x_{q_j}^{\theta_j})$ sends W into $\pi_{x_{q_j}}(W)$, where $\pi_{x_{q_j}}$ is an endomorphism of F_n such that $\pi_{x_{q_j}}(x_i) = x_i$ if $x_{q_j} \neq x_i \in \mathfrak{X}$ and $\pi_{x_{q_j}}(x_{q_j}) = 1$. This contradiction to our assumption that W has the minimum length over all words in $\mathrm{Orb}_{\mathrm{Aut}\, F_n}(W)$ shows that there is no i such that $U_{q_i} \neq V_{q_i}$, thus proving Claim 2. ■

It follows from Claims 1 and 2 that $\varphi|_{F_r} \colon F_r \to F_r$ is an automorphism of F_r. Hence $\varphi(x_1)$ is primitive in F_r and therefore also in F_n. This completes the proof of the theorem. ■

Part II

Polynomial Algebras

Introduction to Part II

This part is about *affine algebraic geometry*, a fascinating area of mathematics that studies polynomials and polynomial mappings. An interesting thing about this area is that most of the research here is focused on five or six outstanding problems. The statements of these problems are rather elementary and can be understood by an average high school student. However, some methods that have been employed so far for attacking those problems are rather sophisticated, and, more importantly, they come from several different areas of mathematics, which stimulates additional interest.

We start right off by giving the statements of five of these problems in the order of decreasing difficulty (in our opinion) and then give some very brief comments, leaving more details to the following chapters. We leave out one of the well-known problems, the Linearization conjecture, because we feel that we do not have sufficient experience with this problem ourselves.

Throughout this part of the book, we denote by $K[x_1, \ldots, x_n]$ the polynomial algebra in n variables over a field K of characteristic 0. More generally, we denote by $K[p_1, \ldots, p_n]$ the subalgebra of $K[x_1, \ldots, x_n]$ generated by polynomials $p_1, \ldots, p_n$.

Problem 1 (the Jacobian conjecture [173]). If for n polynomials $p_1, \ldots, p_n \in K[x_1, \ldots, x_n]$ the corresponding Jacobian matrix is invertible, then $K[p_1, \ldots, p_n] = K[x_1, \ldots, x_n]$.

This is the most famous of the five problems since it cuts across many different areas of mathematics, most notably algebra, algebraic geometry, complex analysis, and dynamical systems. There are several hundred published papers related to this problem, and probably a lot of unpublished

material, because some people may have felt that their research was not conclusive enough to be published. The problem is still open "even" for $n = 2$. It is a common belief that the conjecture is false for $n \geq 3$, but currently available computational resources are insufficient to find a counterexample. It seems plausible that a counterexample will be found within the next few years, when faster computers become available.

On the other hand, the case $n = 2$ appears to be very tantalizing since there are so many partial results in the positive direction that one might get the feeling that a complete positive solution is very close. The other side of this coin is a growing belief that, since so many tools from so many different areas have been tried unsuccessfully, this might be an evidence of the conjecture being false for $n = 2$ as well. In the latter case, it is known that the degrees of polynomials in a counterexample should be over 100, which means it will be a while before we see such a counterexample.

For a general survey and background on this problem, the reader is usually referred to [39], which is, indeed, a good source for results up to 1981. However, in the last 20 years, a great number of new and interesting results have been obtained, and we try to review at least some of them in the relevant chapter of this part of the book. We also refer the reader to a recently published monograph [122].

Problem 2 (the Cancellation conjecture of Zariski). Let R be a commutative algebra over a field of characteristic 0. Suppose $R[x]$ is isomorphic to $K[x_1, \ldots, x_{n+1}]$. Then R is isomorphic to $K[x_1, \ldots, x_n]$ or, in geometric language, let $V \subseteq \mathbb{C}^n$ be a hypersurface. If $V \times \mathbb{C}$ is isomorphic to a hyperplane in $\mathbb{C}^{n+1}$, then V is isomorphic to a hyperplane in $\mathbb{C}^n$.

Note that this problem, as well as many other problems in affine algebraic geometry, admits both algebraic and geometric statements. We shall try to give both versions whenever possible, although we have to tell up front that our methods in this book are purely algebraic and, for the most part, elementary. When a problem is formulated in geometric language, the ground field is usually assumed to be the field of complex numbers.

Unlike the previous problem, the Cancellation conjecture has been settled (affirmatively) in two nontrivial cases: $n = 2$ (Abhyankar, Eakin, and Heinzer [8]) and $n = 3$ (Miyanishi and Sugie [282] and Fujita [138]). It seems reasonable to expect a positive solution for larger values of n as well, but a proof most likely is not going to be easy.

Problem 3 (Nagata's problem). Is every automorphism of $K[x_1, \ldots, x_n]$ tame?

An automorphism of $K[x_1, \ldots, x_n]$ is called *tame* if it is a product of elementary and affine automorphisms. An automorphism of $K[x_1, \ldots, x_n]$ is called *elementary* if it fixes all variables but one.

The answer to this problem is positive for $n = 2$; this is the classical Jung–van der Kulk theorem, which has been improved over the years. The

book [80] probably offers the most comprehensive exposition of this and related results.

When this book was being prepared for publication, Shestakov and Umirbaev [342, 343] gave a (negative) solution of Nagata's problem for $n = 3$ by proving that a particular automorphism of $K[x_1, x_2, x_3]$ (incidentally, suggested by Nagata himself) is not tame. Furthermore, they gave an algorithm for deciding whether or not a given automorphism of $K[x_1, x_2, x_3]$ is tame.

Their proof however cannot be carried on to higher dimensions, and there is still a possibility that the answer to Problem 3 might be positive for $n \geq 4$, although it seems to be a prevalent opinion that the answer should be negative for any $n \geq 3$.

There are only a handful of papers on this very resistant problem, even though there is no lack of allegedly nontame automorphisms for any $n \geq 3$. The reason becomes clear after comparing this problem to the following Problem 4: it is extremely difficult to come up with invariants sensitive enough to distinguish between tame and *stably tame* automorphisms.

Problem 4. Is every automorphism of $K[x_1, \ldots, x_n]$ stably tame?

An automorphism α of $K[x_1, \ldots, x_n]$ is called *stably tame* if the extension of α to some $K[x_1, \ldots, x_N]$, $N \geq n$, by $\alpha\colon x_i \to x_i$, $i > n$, is a tame automorphism of $K[x_1, \ldots, x_N]$.

The answer to this problem is probably affirmative; at least, all known examples of allegedly nontame automorphisms turned out to be stably tame. However, the problem remains open for $n \geq 3$.

To formulate the last of the five problems, we have to introduce some more notation. A polynomial $p \in K[x_1, \ldots, x_n]$ is called a *coordinate polynomial*, or simply a *coordinate*, if $\alpha(p) = x_1$ for some automorphism α of $K[x_1, \ldots, x_n]$. Furthermore, for polynomials $p_1, \ldots, p_m$, by $\langle p_1, \ldots, p_m \rangle$ we denote the ideal of $K[x_1, \ldots, x_n]$ generated by $p_1, \ldots, p_m$ and by $K[x_1, \ldots, x_n]/\langle p_1, \ldots, p_m \rangle$ the corresponding algebra of residue classes.

Problem 5 (the Embedding conjecture of Abhyankar and Sathaye). Let $p \in K[x_1, \ldots, x_n]$, $n \geq 2$. If the algebra $K[x_1, \ldots, x_n]/\langle p \rangle$ is isomorphic to $K[x_1, \ldots, x_{n-1}]$, then p is a coordinate, or, in geometric language, if a hypersurface V in $\mathbb{C}^n$ is isomorphic to the hyperplane $\{x_1 = 0\}$, then it is equivalent to it.

This problem was settled in the affirmative for $n = 2$ in [10] and [380], and it remains open for $n \geq 3$.

In this part of the book, we address Problems 1 through 5 in Chapters 5 through 8.

In the last two chapters, 9 and 10, we treat coordinate polynomials and test polynomials, respectively. These topics were among the focal points of our own research in the last few years. Understanding (and algorithmically

recognizing) coordinate polynomials would be a key to some or all of the five problems above.

Test polynomials, although not as immediately important as coordinate polynomials, appear to be a very attractive subject and have inspired a lot of research recently. They have been formally introduced in [124] as follows: a polynomial $p \in K[x_1, \ldots, x_n]$ is called a *test polynomial* if, whenever one has $\varphi(p) = p$ for a mapping φ of $K[x_1, \ldots, x_n]$ into itself, it follows that φ is an automorphism. Polynomials (and sets of polynomials) with similar properties were earlier considered by Jelonek in [159]. In a more recent paper, Jelonek [163] showed that a generic (in a precise sense) polynomial of degree $> n$ in $\mathbb{C}[x_1, \ldots, x_n]$ is a test polynomial for injective mappings. We discuss this and other results in Chapter 10.

We conclude the Introduction by giving a statement of one of the most important results in affine algebraic geometry, the Abhyankar–Moh theorem [10, Main Theorem]. We have already mentioned one of the corollaries of this result in connection with Problem 5 above. Now we give the result itself:

Theorem 6 ([10]). *Let K be a field of characteristic 0, and let $p = p(x)$, $q = q(x)$ be two polynomials from $K[x]$ of degrees $m \geq 1$ and $n \geq 1$, respectively, such that $K[x] = K[p, q]$. Then either m divides n or n divides m.*

This "innocent-looking" statement turns out to be quite difficult to prove. Several different proofs were published over the years, but none of them were easy. This result now plays a key role in many arguments in affine algebraic geometry; it also plays an important role in this part of our book.

5
The Jacobian Conjecture

In this chapter, we address the most famous of the problems about polynomial mappings:

Problem 5.0.1 (the Jacobian conjecture). If for n polynomials $p_1, \ldots, p_n \in K[x_1, \ldots, x_n]$, the corresponding Jacobian matrix is invertible, then $K[p_1, \ldots, p_n] = K[x_1, \ldots, x_n]$.

This is a very attractive problem because of the simplicity of its statement, which is accessible to a college student, and because there are so many ways to attack it. Commutative algebra, algebraic geometry, real and complex analysis, noncommutative algebra, algebraic topology, and differential algebra have all been used in papers related to the Jacobian conjecture.

The Jacobian conjecture was first formulated by Keller in 1939 (see [173]). It still remains an open problem aside from the trivial case $n = 1$. The case $n = 2$ is discussed in detail in the paper [5] by Abhyankar, where he proves the Galois case. He also shows that the conjecture is equivalent to the curves $p_i = 0$ having only one point at infinity in $\mathbb{P}^2$. He shows that they have at most two points at infinity, a result also proved by Makar-Limanov (unpublished).

By using characteristic pairs and a computer search, Moh [283] proved the conjecture ($n = 2$) if $\deg(p_i) \leq 100$. Campbell [64] proved the Galois case for an arbitrary $n \geq 2$.

Recently, Shpilrain and Yu [363] have proved that φ is an automorphism if J_φ is invertible and for some automorphism ψ of $K[x_1, x_2]$ the composition $\psi\varphi$ fixes a nonconstant polynomial in $K[x_1, x_2]$.

The case $n = 2$ is special also because only for $n \leq 2$ is the group of K-algebra automorphisms of $K[x_1, \ldots, x_n]$ well-understood. For $n = 2$, a well-known theorem of Jung and van der Kulk says that the automorphism group is a free product with amalgamation of two easily described subgroups. Many people think it is "almost certain" that the Jacobian conjecture is true for $n = 2$. For $n > 2$, the prevalent opinion is that the conjecture is false.

Wang [397] proved a remarkable result: when $\deg(p_i) \leq 2$, the Jacobian conjecture is true. The fundamental paper of Bass, Connell, and Wright [39] reduces the Jacobian conjecture to the "cubic homogeneous case". Namely, they proved the following result:

Theorem 5.0.2. *Suppose, for all n and all $F \in (K[x_1, \ldots, x_n])^n$ of the form $F = X + N$ with N cubic homogeneous and $J(N)$ nilpotent, that F is invertible. Then the Jacobian conjecture is true.*

Several alleged proofs of the Jacobian conjecture have been published, including [118], [330], [331], [332], and [334]. For a detailed history of the Jacobian conjecture up to 1981, see [39]. A survey of more recent results can be found in [122].

In the following sections, we give an exposition of our own contribution to this problem.

5.1 Polynomial Retracts and the Jacobian Conjecture

Let $K[x, y]$ be the polynomial algebra in two variables over a field K of characteristic 0. A subalgebra R of $K[x, y]$ is called a *retract* if it satisfies any of the following equivalent conditions:

(R1) There is an idempotent homomorphism (a *retraction*, or *projection*) $\varphi\colon K[x, y] \to K[x, y]$ such that $\varphi(K[x, y]) = R$.

(R2) There is a homomorphism $\varphi\colon K[x, y] \to R$ that fixes every element of R.

(R3) $K[x, y] = R \oplus I$ for some ideal I of the algebra $K[x, y]$.

(R4) $K[x, y]$ is a projective extension of R in the category of K-algebras. In other words, there is a split exact sequence $1 \to I \to K[x, y] \to R \to 1$, where I is the same ideal as in (R3) above.

Examples: K; $K[x, y]$; any subalgebra of the form $K[p]$, where $p \in K[x, y]$ is a *coordinate* polynomial (i.e., $K[p, q] = K[x, y]$ for some polynomial $q \in K[x, y]$). There are other, less obvious examples of retracts: if $p = x + x^2 y$, then $K[p]$ is a retract of $K[x, y]$, but p is not coordinate since it has a fiber

$\{p = 0\}$ that is reducible and therefore is not isomorphic to a line. Even less obvious examples are retracts generated by $p = xy$ or $p = x^2 - y^2$.

The very presence of several equivalent definitions of retracts shows how natural these objects are. Later on, we shall also comment on a very natural geometric meaning of retracts.

In [84], Costa has proved that every proper retract of $K[x, y]$ (i.e., one different from K and $K[x, y]$) has the form $K[p]$ for some polynomial $p \in K[x, y]$ (i.e., it is isomorphic to a polynomial K-algebra in one variable). A natural problem now is to characterize somehow those polynomials $p \in K[x, y]$ that generate a retract of $K[x, y]$. Since the image of a retract under any automorphism of $K[x, y]$ is again a retract, it would be reasonable to characterize retracts up to an automorphism of $K[x, y]$ (i.e., up to a "change of coordinates"). We gave an answer to this problem by proving the following:

Theorem 5.1.1 ([363]). *Let $K[p]$ be a retract of $K[x, y]$. Then there is an automorphism ψ of $K[x, y]$ that takes the polynomial p to $x + y \cdot q$ for some polynomial $q = q(x, y)$. A retraction for $K[\psi(p)]$ is given then by $x \to x + y \cdot q$; $y \to 0$.*

Geometrically, our Theorem 5.1.1 says that (when $K = \mathbb{C}$) every polynomial retraction of a plane is a "parallel" projection (sliding) on a fiber of a coordinate polynomial (which is isomorphic to a line) along the fibers of another polynomial (which generates a retract of $K[x, y]$).

Our proof of this result is based on the well-known Abhyankar–Moh theorem (see Theorem 6). We note in passing that Theorem 5.1.1 also yields a characterization of retracts of a free associative algebra $K\langle x, y\rangle$ if one uses a natural lifting. In Section 5.2, we also make an observation on retracts of a polynomial algebra in arbitrarily many variables (Proposition 5.2.1).

Theorem 5.1.1 yields another useful characterization of retracts of $K[x, y]$:

Corollary 5.1.2. *A polynomial $p \in K[x, y]$ generates a retract of $K[x, y]$ if and only if there is a polynomial mapping of $K[x, y]$ that takes p to x. The "if" part is actually valid for a polynomial algebra in arbitrarily many variables.*

Theorem 5.1.1 has several interesting applications, in particular to the Jacobian conjecture. We establish a link between retracts of $K[x, y]$ and the Jacobian conjecture by means of the following:

Conjecture 5.1.3 (Conjecture "R"). If for a pair of polynomials $p, q \in K[x, y]$ the corresponding Jacobian matrix is invertible, then $K[p]$ is a retract of $K[x, y]$.

This statement is formally much weaker than the Jacobian conjecture since, instead of asking for p to be a coordinate polynomial, we only ask for p to generate a retract, and this property is much less restrictive, as can be

seen from our Theorem 5.1.1. However, the point is that these conjectures are actually equivalent:

Theorem 5.1.4. *Conjecture "R" implies the Jacobian conjecture.*

There are several different ways of proving Theorem 5.1.4 using the characterization of retracts given in Theorem 5.1.1; we believe that the proof we give here (using Newton polygons) is particularly simple.

As a corollary, we show that the Jacobian conjecture is equivalent to other (formally) weaker statements:

Corollary 5.1.5. *Either of the following claims is equivalent to the Jacobian conjecture. Suppose* (p, q) *is a Jacobian pair. Then:*

(i) *for some coordinate polynomial* g, $K[x, y] = K[p] + \langle g \rangle$, *where* $\langle g \rangle$ *is the ideal of* $K[x, y]$ *generated by the polynomial* g;

(ii) *for some coordinate polynomial* g, $K[x, y] = K[g] + \langle p \rangle$.

Corollary 5.3.1 in Section 5.3 also seems interesting since it improves several known partial results on two-variable Jacobian conjecture.

Conjecture "R" has the following geometric interpretation. Suppose we have a polynomial $p \in \mathbb{C}[x, y]$ that has a Jacobian mate. Then every fiber $\{p = c,\ c \in \mathbb{C}\}$ is a nonsingular curve in the complex plane. Moreover, by a result of Kaliman [167], we can restrict our attention to the situation where every fiber of p is irreducible.

If there is another polynomial fiber $\{h = c_0\}$ that is isomorphic to a line and intersects every fiber of p at exactly one point, then we can arrange a geometric projection of the plane onto the curve $\{h = c_0\}$ by sliding a point on a fiber $\{p = c\}$ toward the intersection point of $\{p = c\}$ with $\{h = c_0\}$. This geometric projection will also be algebraic (i.e., $\mathbb{C}[p]$ will be a retract of $\mathbb{C}[x, y]$ in this case).

The only problem is to show that there is a fiber (isomorphic to a line) that intersects every fiber of p at *exactly* one point. In particular, we have:

Corollary 5.1.6 (see [148]). *Suppose* φ *is a polynomial mapping of* $\mathbb{C}[x, y]$ *with an invertible Jacobian matrix. If* φ *is injective on some line, then* φ *is an automorphism.*

We note here that the aforementioned result of Kaliman [167] calls for an example of a noncoordinate polynomial $p \in \mathbb{C}[x, y]$ that has a nonvanishing gradient and all of whose fibers are irreducible. A series of polynomials like that has been constructed in [18].

We also note that if we replaced the condition on a polynomial $p(x, y)$ to have a Jacobian mate by a weaker condition to have a nonvanishing gradient, then Conjecture "R" would not be true. The following counterexample has been communicated to us by A. van den Essen: $p(x, y) = x + (x + x^2 y)^2$.

Another application of retracts to the Jacobian conjecture (although somewhat indirect) is based on the "φ^∞-trick" familiar in combinatorial

group theory (see [383]). For a polynomial mapping $\varphi : K[x,y] \to K[x,y]$, denote by $\varphi^\infty(K[x,y]) = \bigcap_{k=1}^\infty \varphi^k(K[x,y])$ the *stable image* of φ. Then we have:

Theorem 5.1.7. *Let φ be a polynomial mapping of $K[x,y]$. If the Jacobian matrix of φ is invertible, then either φ is an automorphism or $\varphi^\infty(K[x,y]) = K$.*

Our proof of Theorem 5.1.7 is based on recent results of Formanek [133] and Connell and Zweibel [83]. The result of Lemma 5.3.2, which is crucial for our proof of the theorem, seems to be of independent interest.

Obviously, if φ fixes a polynomial $p \in K[x,y]$, then $p \in \varphi^\infty(K[x,y])$. Therefore, we have:

Corollary 5.1.8. *Suppose φ is a polynomial mapping of $K[x,y]$ with an invertible Jacobian matrix. If $\varphi(p) = p$ for some nonconstant polynomial $p \in K[x,y]$, then φ is an automorphism.*

This yields the following interesting reformulation of the Jacobian conjecture: if φ is a polynomial mapping of $K[x,y]$ with an invertible Jacobian matrix, then for some automorphism α, the mapping $\alpha \cdot \varphi$ fixes a nonconstant polynomial.

5.2 Retracts of $K[x,y]$

We start with the following proof:

Proof of Theorem 5.1.1. Let $K[p]$, $p \in K[x,y]$, be a retract of $K[x,y]$ (note that, by a result of Costa [84], every retract of $K[x,y]$ has this form).

Let the corresponding retraction be given by $\varphi\colon x \to q_1(p)$; $y \to q_2(p)$ for some one-variable polynomials q_1, q_2.

Since φ is a retraction, polynomials $q_1(p), q_2(p)$ should generate $K[p]$. Suppose q_1 and q_2 have degree $n \geq 1$ and $m \geq 1$, respectively. Then, by the Abhyankar–Moh theorem (Theorem 6), either n divides m or m divides n. Suppose $\deg(q_1) = k \cdot \deg(q_2)$ for some integer $k \geq 1$.

Then we make the following change of coordinates: $x \to \tilde{x} = x - c \cdot y^k$; $y \to \tilde{y} = y$, where the coefficient $c \in K^*$ is chosen so that in the polynomial $q_1 - c \cdot q_2^k$ the leading terms will cancel out.

In these new coordinates, our retraction acts as follows: $\varphi\colon \tilde{x} \to q_1 - c \cdot q_2^k = \tilde{q}_1$; $\tilde{y} \to q_2 = \tilde{q}_2$. Polynomials $\tilde{q}_1$ and $\tilde{q}_2$ are easily seen to be another generating set of $K[p]$, but the sum of degrees of $\tilde{q}_1$ and $\tilde{q}_2$ is less than that of q_1 and q_2.

Continuing this process, we shall eventually arrive at a pair of polynomials one of which is a constant $c \in K$. Denote the other one by h; then we must have $K[h] = K[p]$ (i.e., $h = c_1 \cdot p + c_2$ for some $c_1 \in K^*$, $c_2 \in K$).

Thus, we have shown that for some automorphism $\psi \in \mathrm{Aut}(K[x,y])$ ("change of coordinates") the composition $\varphi\psi$ takes x to $c_1 \cdot p + c_2$ and y to c. It follows that $c_1 \cdot \psi(p(x,y)) + c_2 = x + (y-c) \cdot q(x,y)$ for some polynomial $q(x,y)$. Applying a linear transformation completes the proof. ■

Proof of Corollary 5.1.2.

(1) Suppose $p \in K[x,y]$ generates a retract of $K[x,y]$. Then, by Theorem 5.1.1, for some automorphism $\psi \in \mathrm{Aut}(K[x,y])$, the polynomial $\psi(p)$ has the form $x + y \cdot q(x,y)$. Let φ be a mapping of $K[x,y]$ that takes x to x; y to 0. Then $\varphi(\psi(p)) = x$.

(2) We are going to prove the "if" part for a polynomial algebra $K[x_1,\ldots,x_n]$ in arbitrarily many variables.

Let $\varphi(p) = x_1$. Consider the following mapping of $K[x_1,\ldots,x_n]$: $\psi\colon x_1 \to p$; $x_i \to 0$, $i = 1,\ldots,n$. Then

$$\psi(\varphi(p)) = p. \tag{5.1}$$

Denote $\varrho = \psi\varphi$. Then, by (5.1), $\varrho(p) = p$, which means ϱ fixes every element of $K[p]$. Also, it is clear that $\varrho(K[x_1,\ldots,x_n]) = K[p]$. Therefore, ϱ is a retraction of $K[x_1,\ldots,x_n]$ and $K[p]$ a retract. ■

We conclude this section with an observation on retracts of a polynomial algebra in arbitrarily many variables.

Proposition 5.2.1. *Let R be a proper retract of $K[x_1,\ldots,x_n]$ generated by polynomials $p_1,\ldots,p_n$, $n \geq 2$. Then $p_1,\ldots,p_n$ are algebraically dependent.*

Proof. Let $\varphi\colon K[x_1,\ldots,x_n] \to R$ be a retraction so that $\varphi(R) = R$. In particular, φ restricted to R is an automorphism of R. If polynomials $p_1,\ldots,p_n$ were algebraically independent, then a result of [83] would imply that φ is an automorphism of $K[x_1,\ldots,x_n]$ as well. In that case, we would have $R = K[x_1,\ldots,x_n]$, which means R is not a proper retract and hence a contradiction. ■

We note that it is an open problem whether or not any retract of $K[x_1,\ldots,x_n]$, $n \geq 3$, can be generated by algebraically independent polynomials. This problem is related to (some forms of) the cancellation problem — see [84] for discussion.

5.3 Applications to the Jacobian Conjecture

First we prove that our conjecture "R" implies the Jacobian conjecture.

Proof of Theorem 5.1.4. Let $\varphi\colon x \to p(x,y)$; $y \to q(x,y)$ be a polynomial mapping of $K[x,y]$ with an invertible Jacobian matrix.

If we assume that our conjecture "R" is true, then $p(x,y)$ generates a retract of $K[x,y]$; hence, by Theorem 5.1.1, for some automorphism $\psi \in$

$\mathrm{Aut}(K[x,y])$, polynomial $\psi(p)$ has the form $x+y\cdot h(x,y)$. Therefore, upon combining φ with ψ if necessary, we may assume that $p(x,y)$ itself has this form.

Now we appeal to a result of [17] (see also [201]) concerning Newton polygons of a Jacobian pair $(p(x,y),q(x,y))$. The Newton polygon of a polynomial $f=f(x,y)=\sum a_{ij}x^iy^j$ is the convex hull of $\{(i,j)\mid a_{ij}\neq 0\}\cup\{(0,0)\}$.

The result of [17] we need is that if $(p(x,y),q(x,y))$ is a Jacobian pair, but $\varphi\colon x\to p(x,y);\ y\to q(x,y)$ is not an automorphism, then Newton polygons of $p(x,y)$ and $q(x,y)$ are radially similar.

Now, by way of contradiction, suppose φ is not an automorphism. Look at the Newton polygon of $p(x,y)$. We see that it has an edge of length 1 — namely, the one between the vertices (0,0) and (1,0). It follows that the similarity ratio for Newton polygons of $p(x,y)$ and $q(x,y)$ is an integer; in particular, $q(x,y)$ has the form $\sum_{i=1}^{k}c_ix^i+y\cdot f(x,y)$ for some $c_i\in K$, $c_k\neq 0$.

Then replace the pair (p,q) with $(p,q-c_kp^k)$. This new pair clearly has the same properties as (p,q) does: it is a Jacobian pair, but the corresponding mapping is not an automorphism. However, the highest degree of monomials of the form x^m in the second polynomial has been decreased.

Therefore, we can repeatedly apply our argument (note that $p(x,y)$ does not change) until we get a pair (p,g), where g has no monomials of the form x^m. But, in that case, the Newton polygon of g has no edges along the x-axis; hence Newton polygons of p and g cannot be radially similar. This contradiction completes the proof of Theorem 5.1.4. ■

Proof of Corollary 5.1.5.

(i) Without loss of generality, we may assume that both p and g have zero constant term. Moreover, upon applying an automorphism to all polynomials under consideration if necessary, we may assume $g=x$.

First we show that if $K[x,y]=K[p]+\langle x\rangle$, then the sum is actually direct.

By way of contradiction, suppose we have

$$x\cdot u=\sum_{i=1}^{m}c_i\cdot p^i \tag{5.2}$$

for some nonzero polynomial $u=u(x,y)$ and constants $c_i\in K$. Since the left-hand side of (5.2) is divisible by x, the right-hand side should be divisible by x, too. This is only possible if p itself is divisible by x, but, in that case, the Newton polygon of p would not have an edge along the y-axis, which contradicts p having a Jacobian mate (see, e.g., [201]).

Thus, we have shown that $K[x,y]=K[p]\oplus\langle x\rangle$. By the definition (R3) of a retract, this implies $K[p]$ is a retract of $K[x,y]$. Therefore, by our Theorem 5.1.4, $K[p,q]=K[x,y]$.

(ii) Arguing as in (i), we get $p \cdot u = \sum_{i=1}^{m} c_i \cdot x^i$. In this case, p cannot depend on y, so $p = p(x)$; but then the equality $K[x, y] = K[x] + \langle p \rangle$ is not possible.

Thus, $K[x, y] = K[x] \oplus \langle p \rangle$. This clearly implies $p = c \cdot y$ for some $c \in K^*$. The result follows. ∎

Corollary 5.3.1. *Let K be an algebraically closed field, and let (p, q), $p, q \in K[x, y]$, be a Jacobian pair. Suppose p has the form $p = x + g$ for some $g \in K[x, y]$ that is divisible by a homogeneous polynomial. Then $K[p, q] = K[x, y]$.*

Proof. If p is linear, then we are done. Suppose p is nonlinear, and suppose g is divisible by a nonconstant homogeneous polynomial h.

If h is divisible by x, then p itself is divisible by x. In that case, the Newton polygon of p does not have an edge along the y-axis, which contradicts p having a Jacobian mate (see [201]).

If h is divisible by y, then $K[p]$ is a retract of $K[x, y]$. If not, then there is $c \in K^*$ such that the homomorphism $x \to p$; $y \to cp$ takes h to 0. This is obviously a retraction, so again $K[p]$ is a retract of $K[x, y]$.

Applying Theorem 5.1.4 yields the result. ∎

Van den Essen and Tutaj [125] have shown that if a Jacobian pair (p, q) is of the form $(x + h_1,\ y + h_2)$, where *both* h_1 and h_2 are homogeneous polynomials, then $K[p, q] = K[x, y]$. It is notable that our Corollary 5.3.1 not only relaxes the condition on the form of polynomials but, most importantly, our condition is imposed on *one* polynomial only.

To prove Theorem 5.1.7, we need the following result of independent interest:

Lemma 5.3.2. *Let $\varphi\colon x \to p(x, y);\ y \to q(x, y)$ be a polynomial mapping of $K[x, y]$ with an invertible Jacobian matrix. Suppose $\varphi(K[x, y])$ contains a coordinate polynomial. Then φ is an automorphism.*

Proof. Upon composing φ with an automorphism if necessary, we may assume that $x \in \varphi(K[x, y])$. This implies $K[p, q, x] = K[p, q]$ and, therefore, $K(p, q, x) = K(p, q)$, where $K(p, q)$ is the quotient field of $K[p, q]$.

On the other hand, by a result of [133], (p, q) being a Jacobian pair implies $K(p, q, x) = K(x, y)$.

Therefore, we have $K(p, q) = K(x, y)$, which by Keller's theorem [173] implies $K[p, q] = K[x, y]$. ∎

Proof of Theorem 5.1.7. Suppose φ is *not* an automorphism. Then, by Lemma 5.3.2, $\varphi(K[x, y])$ contains no coordinate polynomials. In particular, the degree of any polynomial in $\varphi(K[x, y])$ is at least 2. By using inductive argument, we are going to show now that the degree of any nonconstant polynomial in $\varphi^k(K[x, y])$ is at least $(k + 1)$; this will imply $\varphi^\infty(K[x, y]) = K$.

Consider an algebra $\varphi^k(K[x,y])$ for some $k \geq 1$. Since φ is injective (this is ensured by the Jacobian condition), polynomials $\varphi^k(x)$ and $\varphi^k(y)$ are algebraically independent.

If φ restricted to $\varphi^k(K[x,y])$ were an automorphism of $\varphi^k(K[x,y])$, then, by a result of [83], φ would be an automorphism of $K[x,y]$, contrary to our assumption. (Note that $\varphi^k(K[x,y])$ is invariant under φ since, by induction, $\varphi^k(K[x,y]) \subseteq \varphi^{k-1}(K[x,y])$ implies $\varphi^{k+1}(K[x,y]) \subseteq \varphi^k(K[x,y])$.) Hence, $\varphi\,|_{\varphi^k(K[x,y])}$ is not an automorphism of $\varphi^k(K[x,y])$, and our previous argument yields that $\varphi^{k+1}(K[x,y])$ contains no coordinate polynomials of $\varphi^k(K[x,y])$. In particular, the degree of any polynomial in $\varphi^{k+1}(K[x,y])$ is greater than that of any coordinate polynomial in $\varphi^k(K[x,y])$. This completes the induction. ■

In the case $K = \mathbb{C}$, a more complicated (geometric) proof of the result of Theorem 5.1.7 was given by Kraft [184], who also proved that if a polynomial mapping φ of $\mathbb{C}[x,y]$ is *not* birational (i.e., φ does not induce an automorphism of the quotient field $\mathbb{C}(x,y)$), then the stable image of φ is a retract of $\mathbb{C}[x,y]$. This yields a natural question — is the same true for *any* polynomial mapping? (See [383].)

6

The Cancellation Conjecture

In this chapter, we address another famous problem:

Conjecture 6.0.1 (the Cancellation conjecture). Let R be a commutative algebra over a field of characteristic 0. Suppose $R[x]$ is isomorphic to $K[x_1, \ldots, x_{n+1}]$. Then R is isomorphic to $K[x_1, \ldots, x_n]$, or, in geometric language: let $V \subseteq \mathbb{C}^n$ be a hypersurface. If $V \times \mathbb{C}$ is isomorphic to a hyperplane in $\mathbb{C}^{n+1}$, then V is isomorphic to a hyperplane in $\mathbb{C}^n$.

Here we are going to establish a connection between this problem and another well-known problem, the Embedding conjecture of Abhyankar and Sathaye (see Chapter 8), by introducing an "intermediate" conjecture (a precise meaning of this will be clear below). For future reference, we shall call it "the Stable coordinate conjecture". We have to introduce some more notation first.

We focus here on the case $K = \mathbb{C}$. Any collection of polynomials $p_1, \ldots, p_m$ from $\mathbb{C}[x_1, \ldots, x_n]$ determines an algebraic variety $\{p_i = 0,\ i = 1, \ldots, m\}$ in the affine space $\mathbb{C}^n$. We shall denote this algebraic variety by $V(p_1, \ldots, p_m)$.

We say that two algebraic varieties $V(p_1, \ldots, p_m)$ and $V(q_1, \ldots, q_k)$ are *isomorphic* if the algebras of residue classes $\mathbb{C}[x_1, \ldots, x_n]/\langle p_1, \ldots, p_m \rangle$ and $\mathbb{C}[x_1, \ldots, x_n]/\langle q_1, \ldots, q_k \rangle$ are isomorphic. Here $\langle p_1, \ldots, p_m \rangle$ denotes the ideal of $\mathbb{C}[x_1, \ldots, x_n]$ generated by $p_1, \ldots, p_m$. Thus, the isomorphism that we consider here is algebraic, not geometric (i.e., we actually consider isomorphism of what is called *affine schemes*).

On the other hand, we say that two algebraic varieties $V(p_1, \ldots, p_m)$ and $V(q_1, \ldots, q_k)$ are *equivalent* if there is an automorphism of $\mathbb{C}^n$ that

takes one of them onto the other. Algebraically, this means there is an automorphism of $\mathbb{C}[x_1, \ldots, x_n]$ that takes the ideal $\langle p_1, \ldots, p_m \rangle$ to the ideal $\langle q_1, \ldots, q_k \rangle$.

Furthermore, a variety equivalent to $V \times \mathbb{C}$ is called a *cylinder*, a variety of the form $\{p = 0\}$ is called a *hypersurface*, and a hypersurface equivalent to $\{x_1 = 0\}$ is called a *hyperplane*. In particular, a *cylindrical hypersurface* in $\mathbb{C}^n$ is a variety of the form $\{p(x_1, \ldots, x_m) = 0\}$, where $m < n$. Then we have:

Conjecture 6.0.2 (the Embedding conjecture of Abhyankar and Sathaye). If a hypersurface $V(p)$ in $\mathbb{C}^n$ is isomorphic to the hyperplane $V(x_1)$, then it is equivalent to it.

Conjecture 6.0.3 (the Stable coordinate conjecture). Let $V \subseteq \mathbb{C}^n$ be a hypersurface. If $V \times \mathbb{C}$ is equivalent to a hyperplane in $\mathbb{C}^{n+1}$, then V is equivalent to a hyperplane in $\mathbb{C}^n$, or, in purely algebraic language: if $p = p(x_1, \ldots, x_n)$ and $\varphi(p) = x_1$ for some automorphism φ of $\mathbb{C}[x_1, \ldots, x_{n+1}]$, then also $\alpha(p) = x_1$ for some automorphism α of $\mathbb{C}[x_1, \ldots, x_n]$.

The focus of this chapter is actually on Conjecture 6.0.3. It looks similar to the Cancellation conjecture 6.0.1; the difference is that isomorphism here is replaced by equivalence.

All the three conjectures seem to be related; however, it is not so easy to pinpoint precise relations among them. Here we start with the following simple observation.

Proposition 6.0.4.

(a) *Conjectures 6.0.1 and 6.0.2 together imply Conjecture 6.0.3.*

(b) *Conjectures 6.0.3 and 6.0.2 together imply Conjecture 6.0.1.*

(c) *Conjecture 6.0.3 is true for* $n = 2$ *and* 3.

Our proof of part (c) in the case $n = 3$ is based on deep results cited above, whereas the case $n = 2$ can also be handled by somewhat more elementary methods based on a result of [65].

A much less trivial result is the following straightforward implication:

Theorem 6.0.5 ([236]). *For each particular n, the Stable coordinate conjecture implies the Cancellation conjecture.*

Conjecture 6.0.3 also motivates the following generalization:

Problem 6.0.6 (Stable equivalence problem). Are any two stably equivalent polynomials equivalent? Or, in geometric language: is it true that equivalence of two cylindrical hypersurfaces $V(p) \times \mathbb{C}$ and $V(q) \times \mathbb{C}$ in $\mathbb{C}^{n+1}$ implies equivalence of their bases $V(p)$ and $V(q)$ in $\mathbb{C}^n$?

A weaker version of this problem is still quite hard:

Problem 6.0.7. Is it true that equivalence of two cylindrical hypersurfaces $V(p) \times \mathbb{C}$ and $V(q) \times \mathbb{C}$ in $\mathbb{C}^{n+1}$ implies isomorphism of their bases $V(p)$ and $V(q)$ in $\mathbb{C}^n$?

A generalization of Conjecture 6.0.3 in another direction is:

Problem 6.0.8. Can a cylinder in $\mathbb{C}^n$ be equivalent to a noncylinder in $\mathbb{C}^n$ under an automorphism of $\mathbb{C}^m$, $m > n$?

Problem 6.0.6 is, in our opinion, the most interesting one, and it probably holds the key to many mysteries of affine algebraic geometry.

We show here that the answer to Problem 6.0.6 is affirmative in the two-variable case (Theorem 6.0.11). We also show that for $n \geq 3$, the answer is affirmative for two rather large classes of polynomials (Proposition 6.0.9 and Theorem 6.0.10). The first result is just a simple observation:

Proposition 6.0.9. *Let $p = p(x_1, \ldots, x_n)$ be of the form $x_1^{M_1} \cdot \cdots \cdot x_n^{M_n} + \sum_j c(j) \cdot x_1^{i_1(j)} \ldots x_n^{i_n(j)}$, where $c(j)$ are some coefficients, all $M_i > 0$, all monomials under the sum are different from $x_1^{M_1} \cdot \cdots \cdot x_n^{M_n}$, and, for every k, j, one has $i_k(j) \leq M_k$. Then any polynomial $q = q(x_1, \ldots, x_n)$ stably equivalent to p is equivalent to it, or, in geometric language: for any hypersurface $V(q)$ in $\mathbb{C}^n$, equivalence of $V(p) \times \mathbb{C}$ and $V(q) \times \mathbb{C}^k$ in $\mathbb{C}^{n+k}$ implies equivalence of $V(p)$ and $V(q)$ in $\mathbb{C}^n$.*

We note that if p is a coordinate in $\mathbb{C}[x_1, \ldots, x_n]$, then p cannot possibly satisfy the condition of Proposition 6.0.9 since, by a result of Hadas [149], all vertices of the Newton polytope of a coordinate polynomial must be on coordinate hyperplanes. Therefore, Proposition 6.0.9 does not settle Conjecture 6.0.3.

On the other hand, it should be pointed out that, even if a given polynomial p does not satisfy the condition of Proposition 6.0.9, there might be an automorphic image of p that does, and then the result will hold for p as well. For example, $p(x, y) = (x + y)^2 y^2$ does not have the form required in Proposition 6.0.9, but it has an automorphic image $q(x, y) = x^2 y^2$ that does. We discuss the two-variable case in more detail after the proof of Proposition 6.0.9.

Another, more interesting class of polynomials for which Problem 6.0.6 has the affirmative answer is given by the following:

Theorem 6.0.10 ([365]). *Suppose a polynomial $p = p(x_1, \ldots, x_n)$ has the following property: if $\psi(p) = p$ for some injective polynomial mapping ψ of $\mathbb{C}[x_1, \ldots, x_n]$, then ψ must be an automorphism of $\mathbb{C}[x_1, \ldots, x_n]$. Then any polynomial $q = q(x_1, \ldots, x_n)$ stably equivalent to p is equivalent to it.*

Polynomials that satisfy the condition of Theorem 6.0.10 are called *test polynomials* for injective polynomial mappings — see [124]. Jelonek [163] showed that a generic polynomial of degree $> n$ in $\mathbb{C}[x_1, \ldots, x_n]$ is a test polynomial for injective mappings. The statement "a generic polynomial of

degree d has a property W" means that there exists a Zariski open dense subset $U \subseteq \mathcal{H}_d$ of the set $\mathcal{H}_d$ of all polynomials of degree d such that every element of U has the property W. Thus, the class of polynomials covered by Theorem 6.0.10 is really large. Still, it does not include any coordinate polynomials, as was observed in [124].

Then, we have a complete solution of Problem 6.0.6 in the two-variable case:

Theorem 6.0.11 ([236]). *If two polynomials $p, q \in K[x, y]$ are stably equivalent, then they are equivalent.*

We can also answer Problem 6.0.8 in the affirmative:

Theorem 6.0.12. *For any $k \geq 1$ and $n \geq k+2$, there is a variety $V \times \mathbb{C}^k$ in $\mathbb{C}^n$ and a noncylinder U in $\mathbb{C}^n$ such that U is equivalent to $V \times \mathbb{C}^k$ in $\mathbb{C}^{2n}$.*

The simplest example (that we know) illustrating Theorem 6.0.12 would be $U = \{x(1 + xy + z^2) = 1\}$ in $\mathbb{C}^3$ and $V = \{xy = 1\}$ in $\mathbb{C}^2$. The varieties U and $V \times \mathbb{C}$ are inequivalent in $\mathbb{C}^3$ but are equivalent in $\mathbb{C}^6$ (in fact, they are equivalent even in $\mathbb{C}^4$).

6.1 Equivalence and Stable Equivalence

Here we give proofs of the statements from the previous section.

Proof of Proposition 6.0.4. We start with part (a). We are going to prove this statement in the following form: if both Conjectures 6.0.1 and 6.0.2 are true for any n, then for any $k \geq 1$, whenever $V \times \mathbb{C}^k$ is equivalent to a hyperplane in $\mathbb{C}^{n+k}$, one has V equivalent to a hyperplane in $\mathbb{C}^n$.

Let $V = V(p)$, $p = p(x_1, \ldots, x_n)$, and suppose that p is a coordinate in $\mathbb{C}[x_1, \ldots, x_N]$, $N = n + k$. Then, in particular, the hypersurface $\{p = 0\}$ in $\mathbb{C}^N$ is isomorphic to $\mathbb{C}^{N-1}$. If Conjecture 6.0.1 is true, this implies that $\{p = 0\}$ in $\mathbb{C}^n$ is isomorphic to $\mathbb{C}^{n-1}$. Now if Conjecture 6.0.2 is true, this implies that p is a coordinate in $\mathbb{C}[x_1, \ldots, x_n]$, and hence V is equivalent to a hyperplane in $\mathbb{C}^n$.

For part (b), let $V = V(p)$, $p = p(x_1, \ldots, x_n)$, and suppose that the hypersurface $\{p = 0\}$ in $\mathbb{C}^N$, $N > n$, is isomorphic to $\mathbb{C}^{N-1}$. If Conjecture 6.0.2 is true, this implies that p is a coordinate in $\mathbb{C}[x_1, \ldots, x_N]$. Then Conjecture 6.0.3 implies that p is a coordinate in $\mathbb{C}[x_1, \ldots, x_n]$ as well. In particular, the hypersurface $\{p = 0\}$ in $\mathbb{C}^n$ is isomorphic to $\mathbb{C}^{n-1}$.

For part (c), we start with $n = 2$. Let $V = V(p)$, $p = p(x_1, x_2)$, and suppose that for some $N \geq 3$, p is a coordinate in $\mathbb{C}[x_1, \ldots, x_N]$. Then, in particular, the hypersurface $\{p = 0\}$ in $\mathbb{C}^N$ is isomorphic to $\mathbb{C}^{N-1}$. Then, by the result of Abhyankar, Eakin, and Heinzer [8] and Miyanishi [281] cited

in the Introduction, the hypersurface $\{p = 0\}$ in $\mathbb{C}^2$ is isomorphic to $\mathbb{C}$. This implies, by the Abhyankar–Moh theorem [10], that p is a coordinate in $\mathbb{C}[x_1, x_2]$.

Now we get to $n = 3$. The proof here is similar. Let $V = V(p)$, $p = p(x_1, x_2, x_3)$. If p is a coordinate in $\mathbb{C}[x_1, \ldots, x_N]$ for some $N > 3$, then also for any $c \in \mathbb{C}$, $p - c$ is a coordinate in $\mathbb{C}[x_1, \ldots, x_N]$. Therefore, for any $c \in \mathbb{C}$, the hypersurface $\{p = c\}$ in $\mathbb{C}^N$ is isomorphic to $\mathbb{C}^{N-1}$. Then, again for any $c \in \mathbb{C}$, the hypersurface $\{p = c\}$ in $\mathbb{C}^3$ is isomorphic to $\mathbb{C}^2$ by the result of Fujita [138] cited in the Introduction. Now this implies, by a recent result of Kaliman [169] (see also [171]), that p is a coordinate in $\mathbb{C}[x_1, x_2, x_3]$, and hence V is equivalent to a hyperplane in $\mathbb{C}^3$. ■

Proof of Theorem 6.0.5 One of the equivalent formulations of the Cancellation conjecture is (see [122, p. 54]): for every locally nilpotent derivation $\mathcal{D}$ of the algebra $K[x_1, \ldots, x_n]$ with a slice s, the kernel $\operatorname{Ker}\mathcal{D}$ is isomorphic to $K[x_1, \ldots, x_{n-1}]$. By Proposition 2.1 of Wright [405], the latter property is equivalent to s being a coordinate, i.e., an automorphic image of x_1.

Thus, we start with an arbitrary locally nilpotent derivation $\mathcal{D}$ of the algebra $K[x_1, \ldots, x_n]$ with a slice s, and we want to prove that s is a coordinate in $K[x_1, \ldots, x_n]$.

Extend $\mathcal{D}$ to $K[x_1, \ldots, x_{n+1}]$ by $\mathcal{D}(x_{n+1}) = 0$. Then $\operatorname{Ker}\mathcal{D}$ in $K[x_1, \ldots, x_{n+1}]$ is $K[x_1, \ldots, x_n]^{\mathcal{D}}[x_{n+1}]$, where $K[x_1, \ldots, x_n]^{\mathcal{D}}$ denotes $\operatorname{Ker}\mathcal{D}$ in $K[x_1, \ldots, x_n]$. Since s is transcendental over $K[x_1, \ldots, x_n]^{\mathcal{D}}$, we have $K[x_1, \ldots, x_n]^{\mathcal{D}}[x_{n+1}]$ isomorphic to $K[x_1, \ldots, x_n]^{\mathcal{D}}[s]$. The latter algebra is equal to $K[x_1, \ldots, x_n]$ by the result of Wright [405, Proposition 2.1].

Thus we get $K[x_1, \ldots, x_{n+1}]^{\mathcal{D}}$ isomorphic to $K[x_1, \ldots, x_n]$, which implies that s is a coordinate in $K[x_1, \ldots, x_{n+1}]$. Since we are under the assumption that the Stable coordinate conjecture holds for this particular n, we conclude that s is a coordinate in $K[x_1, \ldots, x_n]$, and therefore the Cancellation conjecture holds for the same n. ■

Before we get to the proof of Theorem 6.0.11, we have to do some preliminary work.

Let $p, q \in K[x, y]$; $\varphi(p) = q$ for some automorphism φ of $K[x, y, z, \ldots]$.

Let $\varphi(x) = u = u(x, y, z, \ldots)$, $\varphi(y) = v = v(x, y, z, \ldots)$. We are going to prove a stronger statement (Proposition 6.1.1 below) that will imply Theorem 6.0.11.

We call a pair (u, v) of polynomials *z-reduced* if the sum of z-degrees of the two polynomials cannot be reduced by either a (nondegenerate) linear transformation or a transformation of one of the following two types:

(i) $(u, v) \longrightarrow (u + \mu \cdot v^k, v)$ for some $\mu \in K^*$; $k \geq 2$;

(ii) $(u, v) \longrightarrow (u, v + \mu \cdot u^k)$.

When proving Theorem 6.0.11, we can assume, without loss of generality, that the pair $(u(x, y, z, \ldots), v(x, y, z, \ldots))$ is z-reduced.

If (u, v) is a pair of *two-variable* polynomials such that the sum of their degrees cannot be reduced by a transformation of one the above types, then we call this pair *elementary reduced.*

Proposition 6.1.1. *Let $p \in K[x, y]$ be a two-variable polynomial. Let $(u(x, y, z, \dots), v(x, y, z, \dots))$ be a z-reduced pair of algebraically independent polynomials such that both of them actually depend on z. Then, for any $N \in \mathbb{Z}_+$, there is a polynomial $w = w(x, y)$ such that $\deg(p(u(x, y, w, 0, \dots, 0), v(x, y, w, 0, \dots, 0))) > N$.*

In the proof of Proposition 6.1.1, we shall write just $u(x, y, z)$ and $v(x, y, z)$ instead of $u(x, y, z, 0, \dots, 0)$ and $v(x, y, z, 0, \dots, 0)$ to simplify the notation. First we prove

Lemma 6.1.2. *Let $u(x, y, z)$ and $v(x, y, z)$ be algebraically independent. For any $M \in \mathbb{Z}_+$ and $m, n > M$, there is $c \in K$ such that $u(x, y, x^m y^n + c)$ and $v(x, y, x^m y^n + c)$ are algebraically independent.*

Proof. Recall that polynomials $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ are algebraically dependent over K if and only if the Jacobian matrix $D(f_1, \dots, f_m)$ has rank smaller than m.

Assume, by way of contradiction, that for all $c \in K$ the polynomials $u(x, y, x^m y^n + c), v(x, y, x^m y^n + c) \in K[x, y]$ are algebraically dependent. This means that for all $c \in K$, the matrix

$$D(u(x, y, x^m y^n + c), v(x, y, x^m y^n + c)) = D(u, v)|_{(x, y, x^m y^n + c)} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ m x^{m-1} y^n & n x^m y^{n-1} \end{pmatrix}$$

has rank at most 1. Then for all $c \in K$ the 2×3 matrix $D(u, v)|_{(x, y, x^m y^n + c)}$ has rank at most one, which means that all its 2×2 minors are 0. Using the fact that for all $a, b \in K$ the map from K to K definied by $c \mapsto a^m b^n + c$ is surjective, this implies that for all $a, b, c \in K$ all 2×2 minors of $D(u, v)|_{(a, b, c)}$ are 0. Since K is an infinite field, this in turn implies that all 2×2 minors of $D(u, v)$ are 0. Thus, the rank of $D(u, v)$ is at most one and therefore u and v are algebraically dependent over K, a contradiction. ∎

Proof of Proposition 6.1.1 Since both $u(x, y, z)$ and $v(x, y, z)$ actually depend on z and the pair is z-reduced, we can find $m, n > 2N$ and $c \in K$ such that $u(x, y, x^m y^n + c)$ and $v(x, y, x^m y^n + c)$ are algebraically independent (by Lemma 6.1.2) and elementary reduced.

Now we use a result of Shestakov and Umirbaev from [342] which implies, in particular, that, if two polynomials $r(x, y)$ and $s(x, y)$ of degree $> 2N$ are algebraically independent and elementary reduced, then every nonconstant polynomial in the algebra $K[r, s]$ has degree at least $N + 2$. This completes the proof of Proposition 6.1.1. ∎

Now we can get to the

Proof of Theorem 6.0.11 Recall that $\varphi(x) = u = u(x, y, z, \dots)$, $\varphi(y) = v = v(x, y, z, \dots)$. Upon applying an automorphism of $K[x, y]$ to both $p(x, y)$ and $q(x, y)$ if necessary, we may assume that $u(x, y, z, \dots)$ and $v(x, y, z, \dots)$ are z-reduced. Now we have several cases.

Case 1. Both $u(x, y, z, \dots)$ and $v(x, y, z, \dots)$ actually depend on z. Then we can apply Proposition 6.1.1 to get a contradiction in this case.

Case 2. Say, $v(x, y, z, \dots)$ actually depends on z, whereas $u(x, y, z, \dots)$ does not. Let $x^m y^n$ be the highest monomial in $p(x, y)$ with respect to "lexdeg" ordering with $y > x$. This monomial will contain the highest power of z after we plug in u for x and v for y. This highest power of z then cannot cancel out in $p(u, v)$. Therefore, $p(u, v)$ will depend on z, contrary to the assumption $p(u, v) = q(x, y)$.

Case 3. Neither $u(x, y, z, \dots)$ nor $v(x, y, z, \dots)$ depend on z. If there are other variables that either $u(x, y, z, \dots)$ or $v(x, y, z, \dots)$ depend on, then we find ourselves in Case 1 or 2 above. If not, then there is nothing to prove because the restriction of φ to $K[x, y]$ must be an automorphism of $K[x, y]$.

This completes the proof of Theorem 6.0.11. ■

Remark 6.1.3. The crucial technical tool in our proof of Theorem 6.0.11 was Shestakov–Umirbaev's result from [342] that bounds (from below) the degree of polynomials in the subalgebra of $K[x, y]$ generated by two given polynomials. This is (philosophically) similar to "small cancellation" ideas in combinatorial group theory (see e.g. [227]). We note however that in commutative algebra, these ideas cannot be simply carried on to higher dimensions as the following example shows.

Let $\varphi\colon x \to u = x - yt^2z^2$, $y \to v = 1 + tz^2$, $z \to r = z^2$, $t \to s = -xt + yt^2 + yt^3z^2$. Let $p = p(x, y, z, t) = xy + zt$. Then $\varphi(p) = x$, i.e., $x \in K[u, v, r, s]$, even though the degrees of u, v, r, s are at least 2. Similar examples can be constructed with arbitrarily high degrees of u, v, r, s.

This example therefore makes it appear likely that our proof of Theorem 6.0.11 might be difficult to carry on to higher dimensions, but, of course, this does not mean that the result itself does not hold.

We now get to our partial results on Problem 6.0.6 for arbitrary $n \geq 2$.

Proof of Proposition 6.0.9. Let $\varphi(p) = q$ for some automorphism φ of $\mathbb{C}[x_1, \dots, x_N]$, $N > n$. Then all x_i with $i > n$ have to cancel out in $\varphi(p)$. However, because of the presence of the "dominating" monomial $x_1^{M_1} \cdot \dots \cdot x_n^{M_n}$ in p, if there is some x_i with $i > n$ in some of the $\varphi(x_j)$, $1 \leq j \leq n$, then this x_i will not cancel out in $\varphi(p)$. Therefore, none of the $\varphi(x_j)$, $1 \leq j \leq n$, depend on any x_i, $i > n$, in which case the restriction of φ to $\mathbb{C}[x_1, \dots, x_n]$ must be an automorphism of $\mathbb{C}[x_1, \dots, x_n]$. ■

Remark 6.1.4. As we have mentioned before, even if a given polynomial p does not satisfy the condition of Proposition 6.0.9, there might be an automorphic image of p that does, and then the result will hold for p as well.

Here we note that, in the case where p is a two-variable polynomial over $\mathbb{C}$, it is algorithmically possible to find out whether some automorphic image of p has the form required by Proposition 6.0.9. Indeed, Wightwick [401] showed that, if some automorphic image of p has lower degree than p does, then there is a single elementary automorphism that reduces the degree of p. At the same time, it is easy to see that no elementary automorphism can reduce the degree of a polynomial that satisfies the condition of Proposition 6.0.9. Thus, given a polynomial p, we keep applying elementary automorphisms that reduce the degree until the degree becomes irreducible. Then we check if there is a linear or elementary automorphism preserving the degree of the obtained polynomial that produces a polynomial in the form required by Proposition 6.0.9. For more details, we refer to [401].

We conclude this section with

Proof of Theorem 6.0.12. First we give a proof for $k = 1$, $n = 3$ to simplify the notation; then we explain how this proof generalizes easily to arbitrary $k \geq 1$ and $n \geq k + 2$.

We are going to show that $U = \{x(1 + xy + z^2) = 1\}$ is isomorphic to $W = \{xy = 1\}$ in $\mathbb{C}^3$. The latter variety obviously is of the form $V \times \mathbb{C}$, whereas the former is not.

It will be technically more convenient to write algebras of residue classes as "algebras with relations"; i.e., for example, instead of $\mathbb{C}[x_1, \ldots, x_n]/\langle p(x_1, \ldots, x_n)\rangle$ we shall write $\langle x_1, \ldots, x_n \mid p(x_1, \ldots, x_n) = 0\rangle$.

Now we get the following chain of "elementary" isomorphisms:

$$
\begin{aligned}
&\langle x, y, z \mid x(1 + xy + z^2) = 1\rangle \\
&\quad = \langle x, y, z \mid x(1 + xy + z^2) = 1,\ xy(1 + xy + z^2) = y\rangle \\
&\quad = \langle x, y, z \mid x + x^2y + xz^2 = 1,\ xy + x^2y^2 + xyz^2 = y\rangle \\
&\quad \cong \langle x, y, z, u \mid x + x^2y + xz^2 = 1,\ xy + x^2y^2 + xyz^2 = y,\ u = xy\rangle \\
&\quad \cong \langle x, y, z, u \mid x + xu + xz^2 = 1,\ y = u + u^2 + uz^2,\ u = xy\rangle \\
&\quad \cong \langle x, z, u \mid x + xu + xz^2 = 1,\ u = x(u + u^2 + uz^2)\rangle \\
&\quad \cong \langle x, y, z \mid x + xy + xz^2 = 1,\ y = x(y + y^2 + yz^2)\rangle \\
&\quad = \langle x, y, z \mid x + xy + xz^2 = 1\rangle \\
&\quad = \langle x, y, z \mid x(1 + y + z^2) = 1\rangle \\
&\quad \cong \langle x, y, z \mid xy = 1\rangle.
\end{aligned}
$$

Thus, $U = \{x(1 + xy + z^2) = 1\}$ is isomorphic to $W = \{xy = 1\}$ in $\mathbb{C}^3$. Upon replacing U with $U_m = \{x(1 + xy + z_1^2 + \cdots + z_m^2) = 1\}$, where $z_1, \ldots, z_m$ are variables, and using the same chain of "elementary" isomorphisms, we get examples, for any $m \geq 1$, of noncylinders U_m isomorphic to $W = \{xy = 1\}$ in $\mathbb{C}^{m+2}$. Then, upon replacing U_m with $U_{m,r} = \{x \cdot t_1 \cdot \cdots \cdot t_r \cdot (1 + xy + z_1^2 + \cdots + z_m^2) = 1\}$ and W with

$W_r = \{xy \cdot t_1 \cdot \cdots \cdot t_r = 1\}$, where $t_1, \ldots, t_r$ are variables, and using the same chain of isomorphisms, we get the isomorphism of $U_{m,r}$ to W_r in $\mathbb{C}^{m+2+r}$ for any $m \geq 1$, $r \geq 0$.

To show that, for instance, the polynomial $x(1 + xy + z_1^2 + \cdots + z_m^2)$ is not equivalent to any polynomial in less than $(m+2)$ variables, it is clearly sufficient to show the same for the polynomial $q = 1 + xy + z_1^2 + \cdots + z_m^2$. The gradient of the latter polynomial is $(y, x, 2z_1, \ldots, 2z_m)$. Now the "chain rule" for partial derivatives shows that, if we apply an automorphism φ to q, then the gradient of $\varphi(q)$ must contain all the variables $x, y, z_1, \ldots, z_m$. Then the same is true for the polynomial $\varphi(q)$ itself.

Finally, to get the equivalence claimed in the statement of Theorem 6.0.12 out of the isomorphism above, we just recall (see, e.g., [364, Corollary 1.2]) that if two algebraic varieties $V(p_1, \ldots, p_m)$ and $V(q_1, \ldots, q_k)$ in $\mathbb{C}^n$ are isomorphic, then the varieties $V(p_1, \ldots, p_m, x_{n+1}, \ldots, x_{2n})$ and $V(q_1, \ldots, q_k, x_{n+1}, \ldots, x_{2n})$ in $\mathbb{C}^{2n}$ are equivalent under a (tame) automorphism of $\mathbb{C}^{2n}$. ■

6.2 Around Danielewski's Example

In Danielewski's example [88] of two isomorphic cylindrical hypersurfaces $V(p) \times \mathbb{C}$ and $V(q) \times \mathbb{C}$ with nonisomorphic bases $V(p)$ and $V(q)$ in $\mathbb{C}^3$, we have $p = p(x, y, z) = xy - z^2 + 1$; $q = q(x, y, z) = x^2y - z^2 + 1$. We start this section by giving an explicit algebraic isomorphism (due to P. Russell) for cylinders in Danielewski's example. This argument also establishes the fact that Danielewski's cylinders are isomorphic over any ground field of characteristic 0, not just over $\mathbb{C}$. We are grateful to P. Russell for kindly permitting us to use his observation.

Remark 6.2.1 (Russell, unpublished). Let $p = p(x_1, y_1, z_1) = x_1y_1 - z_1^2 + 1$; $q = q(x_2, y_2, z_2) = x_2^2y_2 - z_2^2 + 1$, and let K be an arbitrary field of characteristic 0. The following mapping φ from $K[x_1, y_1, z_1, u]$ to $K[x_2, y_2, z_2, v]$ induces an isomorphism between algebras of residue classes $K[x_1, y_1, z_1, u]/\langle p \rangle$ and $K[x_2, y_2, z_2, v]/\langle q \rangle$: φ: $x_1 \to x_2$; $y_1 \to x_2v^2 + 2z_2v + x_2y_2$; $z_1 \to x_2v + z_2$; $u \to x_2v^3 + 3z_2v^2 + 3x_2y_2v + y_2z_2$.

It is easy to check that φ induces a homomorphism between $K[x_1, y_1, z_1, u]/\langle p \rangle$ and $K[x_2, y_2, z_2, v]/\langle q \rangle$.

We are going to show that φ is *onto*. We already have $x_2 \pmod{\langle q \rangle}$ in the image; a straightforward computation shows that $\varphi(y_1z_1) - x_2 \cdot \varphi(u) = -2x_2^2y_2v + 2z_2^2v = 2v(z_2^2 - x_2^2y_2) = 2v \pmod{\langle q \rangle}$. Thus, we have $v \pmod{\langle q \rangle}$ and therefore also $z_2 \pmod{\langle q \rangle}$ in the image. Now inspection of $\varphi(y_1)$ shows that we have $x_2y_2 \pmod{\langle q \rangle}$ and hence also $x_2^2y_2^2 \pmod{\langle q \rangle}$ in the image. From $\varphi(u)$ we now see that we have $y_2z_2 \pmod{\langle q \rangle}$ and hence also $y_2z_2^2 \pmod{\langle q \rangle}$ in the image. This finally gives $y_2z_2^2 - x_2^2y_2^2 = y_2 \pmod{\langle q \rangle}$ in the image.

Thus, φ is *onto*. If φ were not one-to-one, then the algebra $K[x_2, y_2, z_2, v]/\langle q \rangle$ would be isomorphic to an algebra $K[x_1, y_1, z_1, u]/J$, where J is an ideal that properly contains $\langle p \rangle$. This isomorphism then implies that J can be generated (as an ideal) by a single polynomial. Since p is irreducible, this generating polynomial has to be p.

Therefore, φ is one-to-one and hence an isomorphism.

More generally, by results of Danielewski [88] and Fieseler [130], the hypersurface $D(k) = \{xy^k + z^2 + 1 = 0\}$ is not isomorphic to $D(m) = \{xy^m + z^2 + 1 = 0\}$ in $\mathbb{C}^3$ if $k \neq m$, $k, m \geq 1$, whereas the cylinders $D(k) \times \mathbb{C}$ and $D(m) \times \mathbb{C}$ are isomorphic subvarieties of $\mathbb{C}^4$.

Furthermore, a combination of Danielewski's example with our characterization of isomorphic varieties [364, Corollary 1.2] yields an example of *equivalent* cylinders with inequivalent (even nonisomorphic!) bases; those cylinders, however, are not hypersurfaces:

Proposition 6.2.2. *As in Danielewski's example, let* $p(x, y, z) = xy - z^2 + 1$; $q(x, y, z) = x^2y - z^2 + 1$. *Then the varieties* $V_1 = V(p(x, y, z), t, u, v, w)$ *and* $V_2 = V(q(x, y, z), t, u, v, w)$ *in* $\mathbb{C}^7$ *are not isomorphic, whereas the cylinders* $V_1 \times \mathbb{C}$ *and* $V_2 \times \mathbb{C}$ *are equivalent in* $\mathbb{C}^8$.

Proof. First of all, the varieties $V_1 = V(p(x, y, z), t, u, v, w)$ and $V_2 = V(q(x, y, z), t, u, v, w)$ in $\mathbb{C}^7$ are not isomorphic since if they were, then $V(p(x, y, z))$ and $V(q(x, y, z))$ would be isomorphic in $\mathbb{C}^3$ which is known not to be the case.

On the other hand, we know that the algebras of residue classes $\mathbb{C}[x, y, z, t]/\langle p \rangle$ and $\mathbb{C}[x, y, z, t]/\langle q \rangle$ are isomorphic. This implies, by [364, Corollary 1.2], that the varieties $V(p(x_1, y_1, z_1), u, x_2, y_2, z_2, v)$ and $V(q(x_1, y_1, z_1), u, x_2, y_2, z_2, v)$ are equivalent under an automorphism of $\mathbb{C}^8$. We note that the latter equivalence also follows from a result of Asanuma [28]. ■

Having in mind Danielewski's example and motivated by Theorem 6.0.5, we ask:

Problem 6.2.3. Let $p = p(x, y, z) = xy + z^2$. Is it true that every polynomial in $K[x, y, z]$ which is stably equivalent to p is, in fact, equivalent to p?

Another natural question is whether or not Danielewski's surfaces/cylinders have unique embeddings in $\mathbb{C}^4$. We show here that all but one of them do not:

Proposition 6.2.4. *For any* $m \geq 2$, *the hypersurface* $D(m) \times \mathbb{C}^{k-3} = \{xy^m + z^2 + 1 = 0\}$ *has at least* 2 *inequivalent embeddings in* $\mathbb{C}^k$ *for any* $k \geq 3$.

Proof. We give a proof here for $m = 2$, just to simplify the notation. We get the following chain of "elementary" isomorphisms:

$$\begin{aligned}
&\langle x, y, z \mid xy^2 + z^2 + 1 = 0\rangle \\
&\quad \cong \text{(applying the automorphism } \varphi\colon x \to x,\ y \to y+1,\ z \to z) \\
&\quad \langle x, y, z \mid x = -xy^2 - 2xy - z^2 - 1\rangle \\
&\quad \cong \langle x, y, z, u \mid u = xy,\ x = -uy - 2u - z^2 - 1\rangle \\
&\quad \cong \langle x, y, z, u \mid u = -uy^2 - 2uy - z^2 y - y,\ x = -uy - 2u - z^2 - 1\rangle \\
&\quad \cong \langle y, z, u \mid u = -uy^2 - 2uy - z^2 y - y\rangle \\
&\quad \cong \langle x, y, z \mid x = -xy^2 - 2xy - z^2 y - y\rangle \\
&\quad \cong \text{(applying the automorphism } \varphi\colon x \to x,\ y \to y-1,\ z \to z) \\
&\quad \langle x, y, z \mid xy^2 + z^2 y - z^2 + y - 1 = 0\rangle.
\end{aligned}$$

Now let $p = p(x, y, z) = xy^2 + z^2 + 1$, $q = q(x, y, z) = xy^2 + z^2 y - z^2 + y - 1$. We are going to show that the gradients $\operatorname{grad}(p)$ and $\operatorname{grad}(q)$ have different numbers of zeros. This obviously implies that p and q are inequivalent under any automorphism of $K[x, y, z]$ (in fact, this implies that p and q are even stably inequivalent).

Compute:

$$\begin{aligned}
\operatorname{grad}(p) &= (y^2, 2xy, 2z) \\
\operatorname{grad}(q) &= (y^2, 2xy + z^2 + 1, 2yz - 2z).
\end{aligned}$$

We see that $\operatorname{grad}(p)$ has infinitely many zeros ($y = z = 0$, x arbitrary), whereas $\operatorname{grad}(q)$ has no zeros. This completes the proof. ∎

We note that for $k = 3$, this was also proved in [137] (by an altogether different method). For $m = 1$, the question is open:

Problem 6.2.5. Does the hypersurface $D(1) \times \mathbb{C} = \{xy + z^2 + 1 = 0\}$ have a unique embedding in $\mathbb{C}^4$?

It is also unknown whether $D(1)$ has a unique embedding in $\mathbb{C}^3$ (cf. [137, Question 1]).

We note that Problems 6.2.3 and 6.2.5 cannot both have positive answers. Indeed, if the answer to Problem 6.2.5 was positive, then, since we know that $D(1) \times \mathbb{C}$ is isomorphic to $D(m) \times \mathbb{C}$ for any $m \geq 1$, we would have $D(1) \times \mathbb{C}$ equivalent to $D(m) \times \mathbb{C}$ in $\mathbb{C}^4$. Then, if the answer to Problem 6.2.3 was positive, this would imply that $D(1)$ is equivalent to $D(m)$ in $\mathbb{C}^3$, which is known not to be the case.

This simple trick also works in a more general situation, namely:

Proposition 6.2.6. *Let $V(p)$, $p = p(x_1, \ldots, x_n)$ be a hypersurface in $\mathbb{C}^n$. Suppose that the following two conditions hold:*

(i) *$V(p) \times \mathbb{C}$ has a unique embedding in $\mathbb{C}^{n+1}$.*

(ii) *If $V(p)$ is stably equivalent to $V(q)$ for some $q = q(x_1, \ldots, x_n)$, then $V(p)$ is equivalent to $V(q)$.*

Then, whenever $V(p) \times \mathbb{C}$ is isomorphic to $V(q) \times \mathbb{C}$, it follows that $V(p)$ and $V(q)$ are isomorphic subvarieties of $\mathbb{C}^n$.

The proof is obvious; we omit the details. Equally obvious is the following:

Proposition 6.2.7. *Let $V(p)$, $p = p(x_1, \ldots, x_n)$ be a hypersurface in $\mathbb{C}^n$. Suppose that the following two conditions hold:*

(i) *$V(p)$ has a unique embedding in $\mathbb{C}^n$.*

(ii) *If $V(p) \times \mathbb{C}^s$ and $V(q) \times \mathbb{C}^s$ are isomorphic subvarieties of $\mathbb{C}^{n+s}$ for some $s \geq 1$, then $V(p)$ and $V(q)$ are isomorphic subvarieties of $\mathbb{C}^n$.*

Then, whenever $V(p)$ is stably equivalent to $V(q)$ for some $q = q(x_1, \ldots, x_n)$, one has $V(p)$ equivalent to $V(q)$.

Finally, we make one more observation inspired by Danielewski's example:

Proposition 6.2.8. *Let $y, x_1, \ldots, x_m$, $m \geq 1$, be variables, and let $p = p(x_1, \ldots, x_m)$ be an arbitrary polynomial. Then hypersurfaces $y \cdot p = 1$ and $y \cdot p^k = 1$ are isomorphic in $\mathbb{C}^{m+1}$ for any $k \geq 1$.*

Speaking somewhat informally, adding a polynomial $q(z_1, \ldots, z_k)$ in new variables z_i to both polynomials in the statement of Proposition 6.2.8 can "spoil" this simple but delicate isomorphism (in the course of the proof, we shall see why), but, apparently, sometimes this isomorphism "survives" in higher dimensions — hence the isomorphism of cylinders. Understanding exactly when this happens can be the key to constructing counterexamples to (some of) the conjectures of this chapter.

Proof of Proposition 6.2.8. Here we get the following chain of "elementary" isomorphisms:

$$\begin{aligned}
\langle y, x_1, \ldots, x_m \mid y \cdot p = 1 \rangle &= \langle y, x_1, \ldots, x_m \mid y \cdot p = 1,\ y^2 \cdot p = y \rangle \\
&\cong \langle y, x_1, \ldots, x_m, u \mid y \cdot p = 1,\ y^2 \cdot p = y,\ u = y^2 \rangle \\
&\cong \langle y, x_1, \ldots, x_m, u \mid u \cdot p^2 = 1,\ u \cdot p = y,\ u = u^2 p^2 \rangle \\
&\cong \langle x_1, \ldots, x_m, u \mid u \cdot p^2 = 1,\ u = u^2 p^2 \rangle \\
&= \langle x_1, \ldots, x_m, u \mid u \cdot p^2 = 1 \rangle \\
&\cong \langle y, x_1, \ldots, x_m \mid y \cdot p^2 = 1 \rangle.
\end{aligned}$$

Upon applying the same trick $(k-1)$ times, we will have $y \cdot p = 1$ isomorphic to $y \cdot p^k = 1$. ∎

7

Nagata's Problem

Let K be a field and let $K[X] = K[x_1, \ldots, x_n]$ be the polynomial algebra in n variables $x_1, \ldots, x_n$ over K. Sometimes we prefer to denote the elements of X by x, y, z, etc. In this chapter, we study the group of K-algebra automorphisms $\mathrm{Aut}(K[x_1, \ldots, x_n])$, $n \geq 2$.

The group $\mathrm{Aut}(K[X])$ has two important subgroups. The first one is the group $A(n, K)$ consisting of all affine automorphisms. The other one, $J(n, K)$, is generated by all triangular automorphisms defined as follows. Given invertible elements $a_1, \ldots, a_n$ in K and polynomials $f_i \in K[x_{i+1}, \ldots, x_n]$, $i = 1, \ldots, n$ (f_n is a polynomial in zero variables; i.e., $f_n \in K$), the map $(a_1x_1 + f_1, a_2x_2 + f_2, \ldots, a_nx_n + f_n)$ is called a triangular automorphism of $K[X]$. The group generated by $A(n, K)$ and $J(n, K)$ is the group of *tame* automorphisms and is denoted by $T(n, K)$. The automorphisms of $K[X]$ that are not in $T(n, K)$ are called *wild*. Similarly, one can define tame and wild automorphisms of $K[X]$ when K is any commutative ring with identity.

Finally, an automorphism α of $K[x_1, \ldots, x_n]$ is called *stably tame* if the extension of α to some $K[x_1, \ldots, x_N]$, $N \geq n$, by $\alpha\colon x_i \to x_i$, $i > n$, is a tame automorphism of $K[x_1, \ldots, x_N]$.

Now we state two main problems that we address in this chapter.

Problem 7.0.1. Is it true that $\mathrm{Aut}(K[x_1, \ldots, x_n]) = T(n, K)$; i.e., is every automorphism of $K[x_1, \ldots, x_n]$ tame?

Problem 7.0.2. Is every automorphism of $K[x_1, \ldots, x_n]$ stably tame?

For $n = 2$, Problem 7.0.1 is long known to have an affirmative answer. There are several known proofs of this fact originally obtained by Jung [164] for $K = \mathbb{C}$ and by Van der Kulk [194] for any field K.

When this book was being prepared for publication, Shestakov and Umirbaev [342, 343] gave a negative solution to Problem 7.0.1 for $n = 3$ by proving that a particular automorphism of $K[x, y, z]$ suggested by Nagata back in 1972 (see the next section) is not tame. Furthermore, they gave an algorithm for deciding whether or not a given automorphism of $K[x, y, z]$ is tame.

Theorem 7.0.3. *If one can effectively perform computations in the ground field K of characteristic 0, then there is an algorithm for deciding whether or not a given automorphism of $K[x, y, z]$ is tame.*

Theorem 7.0.4 ([343]). *The following automorphism ν, due to Nagata, of a polynomial algebra $K[x, y, z]$ over a field K of characteristic 0 is wild:*

$$\begin{aligned}\nu(x) &= x - 2y(y^2 + xz) - z(y^2 + xz)^2,\\ \nu(y) &= y + z(y^2 + xz),\\ \nu(z) &= z.\end{aligned}$$

Their proof uses several ingredients, but is ultimately based on the same idea that underlies Whitehead's method (see our Section 1.2). Namely, one has to choose a collection of "basic" automorphisms in such a way that if, for a given (coordinate) polynomial p, its degree can be decreased by a tame automorphism, then it can be, in fact, decreased by a *single* automorphism from your collection. If the latter is effectively verifiable, then you have an algorithm for detecting tameness. In Shestakov–Umirbaev's proof, "basic" automorphisms are compositions of up to four(!) elementary or linear automorphisms (recall that elementary automorphisms are those that change just one variable). This explains technical difficulty of the paper [343].

Later, Umirbaev and Yu [393] used a similar technique to obtain a stronger result:

Theorem 7.0.5 ([393]). *Two components of Nagata's automorphism, $x - 2y(y^2 + xz) - z(y^2 + xz)^2$ and $y + z(y^2 + xz)$, are* wild coordinates; *i.e., neither of them can be a component of a tame automorphism.*

Proofs of all these results cannot be carried on to higher dimensions, and there is still a possibility that the answer to Problem 7.0.1 might be positive for $n \geq 4$, although it seems to be a prevalent opinion that the answer should be negative for any $n \geq 3$.

There are only a handful of papers on this very resistant problem, even though there is no lack of allegedly nontame automorphisms for any $n \geq 3$. The reason becomes clear after comparing this problem to Problem 7.0.2: it is extremely difficult to come up with invariants sensitive enough to distinguish between tame and stably tame automorphisms. We also note

that M. Smith [370] showed that the Nagata automorphism is stably tame and becomes tame if we extend it to an automorphism of $K[x, y, z, t]$ by fixing t.

The answer to Problem 7.0.2 is probably affirmative; at least, all known examples of allegedly nontame automorphisms turned out to be stably tame. However, the problem remains open for $n \geq 3$. There is not much that we can say about Problem 7.0.2 at this time, but the following recent result by Berson seems interesting:

Theorem 7.0.6 ([50]). *Every coordinate of $K[x_1, \ldots, x_n]$ is a component of a tame automorphism of $K[x_1, \ldots, x_N]$ for some $N \geq n$.*

Even though Nagata's automorphism is now proved to be wild, there is still need in new approaches to proving nontameness of particular automorphisms since, as we have mentioned before, Shestakov–Umirbaev's proof cannot be carried on to higher dimensions. In the following two sections, we discuss two possible approaches and use Nagata's automorphism as a "proving ground" since it is the simplest wild automorphism. It turns out that Nagata's automorphism has some properties which distinguish it from known tame automorphisms.

In Section 7.1, we consider Gröbner basis techniques. There is a well-known Gröbner basis algorithm for deciding whether an endomorphism of $K[X]$ is an automorphism and, if the answer is affirmative, finding the inverse. An automorphism of $K[X]$ can be reconstructed from all n^2 face polynomials of its inverse. In the two-variable case, we prove that just two face polynomials are enough, and this result is closely related to the fact that every automorphism of $K[x, y]$ is tame. Examples show that a similar result does not hold for $n \geq 3$. We show that the reduced Gröbner basis of three face polynomials of the Nagata automorphism obtained by substituting $z = 0$ does not produce an automorphism under any "tag" monomial ordering, in contrast to all examples of tame automorphisms of $K[x, y, z]$ that we have tested. Based on this evidence, we formulate a conjecture that, if true, would imply that Nagata's automorphism is wild.

In Section 7.2, we try to lift the Nagata automorphism to an automorphism of the free associative algebra $K\langle x, y, z\rangle$. Obviously, every tame automorphism of $K[X]$ can be lifted to an automorphism of $K\langle X\rangle$. Therefore, although an automorphism of $K[X]$ may not be tame, if it can be lifted to an automorphism of $K\langle X\rangle$, it may be regarded as "not wilder" than the corresponding automorphism of the free algebra. If an automorphism of $K[X]$ cannot be lifted to an automorphism of $K\langle X\rangle$, we may ask the question of "how far" it can be lifted. The natural way to measure the "distance" is in the language of T-ideals (i.e., ideals of $K\langle X\rangle$ that are invariant under all endomorphisms of $K\langle X\rangle$). Recall that, by a result of M. Smith [370], Nagata's automorphism is stably tame; i.e., it becomes tame if we extend it to the polynomial algebra in four variables $K[x, y, z, v]$ assuming that it fixes v. Unfortunately, her procedure does not give a lift-

ing to Aut $K\langle x, y, z, v\rangle$ that fixes v. We have not succeeded in lifting the Nagata automorphism to an automorphism of $K\langle x, y, z\rangle$, but we give an explicit lifting to the algebra $K\langle x, y, z\rangle/C^k$, where C is the commutator ideal of $K\langle x, y, z\rangle$ and k is any positive integer. By a result of Umirbaev [390], such liftings exist for any automorphism of $K[X]$, but our lifting has the advantage that it fixes z as the Nagata automorphism itself does.

7.1 Gröbner Bases and Face Functions

Our exposition in this section follows [106].

A Gröbner basis is a (finite) set of special generators of an ideal of a polynomial algebra. Fixing some ordering of the monomials in $K[x_1, \ldots, x_n]$, the leading term of any element from the ideal is divisible by a leading term of some element from the Gröbner basis. The basis is reduced if no term of its elements is divisible by the leading term of another element. The Gröbner bases have many attractive computational properties. The method is widely used in computational commutative algebra and in computational algebraic geometry. The reader is referred to [13]. The theory of Gröbner bases was used, in particular, for deciding if a given polynomial map $F = (f_1, \ldots, f_n)$ is an automorphism. The algorithm uses "tag" variables in a fashion related to the method for finding the relations among the f_i's. We introduce tag variables, indeterminates $y_1, \ldots, y_n$, one for each f_i. Let $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ have a monomial ordering, where

$$K[x_1, \ldots, x_n] \succ K[y_1, \ldots, y_n],$$

which means that each monomial in $K[x_1, \ldots, x_n]$ is larger than any monomial in $K[y_1, \ldots, y_n]$. We call it a "tag" monomial ordering.

Proposition 7.1.1. *Let $F = (f_1, \ldots, f_n)$ be an endomorphism of $K[x_1, \ldots, x_n]$. Then F is an automorphism if and only if the ideal I of $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ generated by*

$$\{y_1 - f_1(x_1, \ldots, x_n), \ldots, y_n - f_n(x_1, \ldots, x_n)\}$$

has a generating set of the form

$$\{x_1 - g_1(y_1, \ldots, y_n), \ldots, x_n - g_n(y_1, \ldots, y_n)\}.$$

Moreover, $G := G(X) := (g_1(X), \ldots, g_n(X))$ is the inverse of $F = (f_1, \ldots, f_n)$ and the reduced Gröbner basis of the ideal I with respect to any "tag" monomial ordering $\succ$ such that $K[x_1, \ldots, x_n] \succ K[y_1, \ldots, y_n]$ is precisely $\{x_1 - g_1(y_1, \ldots, y_n), \ldots, x_n - g_n(y_1, \ldots, y_n)\}$.

There are several proofs of this result, by van den Essen [119] and Shannon and Sweedler [335] for fields and Abhyankar and Li [9] for arbitrary commutative rings K.

It has been proved by several authors (see McKay and Wang [242], Li [216], van den Essen and Kwiecinski [123], and Yu [409]) that a polynomial map $F = (f_1, \ldots, f_n) \in \mathrm{Aut}(K[x_1, \ldots, x_n])$ is completely determined by its n^2 face polynomials

$$f_1(0, x_2, \ldots, x_n), \ldots, f_1(x_1, \ldots, x_{n-1}, 0),$$

$$\ldots$$

$$f_n(0, x_2, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_{n-1}, 0).$$

Now we present a result concerning the reduced Gröbner bases of the face functions. It is more general than that by van den Essen [119].

Proposition 7.1.2. *Let K be any field and $F = (f_1, \ldots, f_n) \in \mathrm{Aut}(K[x_1, \ldots, x_n])$. Let*

$$G = \{x_1 - g_1(y_1, \ldots, y_n), \ldots, x_n - g_n(y_1, \ldots, y_n)\}$$

be the reduced Gröbner basis of the ideal $I = (y_1 - f_1(x_1, \ldots, x_n), \ldots, y_n - f_n(x_1, \ldots, x_n))$ in $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ with respect to any "tag" monomial ordering $\succ$ such that $K[x_1, \ldots, x_n] \succ K[y_1, \ldots, y_n]$. Then, for any integer $j = 1, \ldots, n$, the set

$$H = \{x_1 - g_1(y_1, \ldots, y_n), \ldots, x_{j-1} - g_{j-1}(y_1, \ldots, y_n), g_j(y_1, \ldots, y_n), \\ x_{j+1} - g_{j+1}(y_1, \ldots, y_n) \ldots, x_n - g_n(y_1, \ldots, y_n)\}$$

is a Gröbner basis of the ideal J generated by

$$\{y_1 - f_1(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n), \ldots, \\ y_n - f_n(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n)\}.$$

In general, H is not the reduced Gröbner basis. The reduced Gröbner basis is obtained after reduction of all polynomials $g_i(y_1, \ldots, y_n)$, $i = 1, \ldots, \hat{\jmath}, \ldots, n$, by $g_j(y_1, \ldots, y_n)$. (Here $\hat{\jmath}$ means that the corresponding number j does not occur in the expression.)

Proof. The sets

$$\{y_i - f_i(x_1, \ldots, x_n) \mid i = 1, \ldots, n\}, \quad \{x_i - g_i(y_1, \ldots, y_n) \mid i = 1, \ldots, n\}$$

generate the same ideal I of $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$. Substituting $x_j = 0$, we obtain that the set H generates in $K[x_1, \ldots, \hat{x}_j, \ldots, x_n, y_1, \ldots, y_n]$ the same ideal as

$$\{y_1 - f_1(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n), \ldots, \\ y_n - f_n(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n)\}.$$

Hence these two sets generate also the same ideal in $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$. The set H is a Gröbner basis because every element from the ideal J is a linear combination of polynomials with leading term containing

$x_1, \ldots, \hat{x}_j, \ldots, x_n$ and of polynomials divisible by $g_j(y_1, \ldots, y_n)$. After reduction of all polynomials $g_i(y_1, \ldots, y_n)$, $i = 1, \ldots, \hat{j}, \ldots, n$, by $g_j(y_1, \ldots, y_n)$, we obtain a set $\bar{H}$ such that no monomial of an element from $\bar{H}$ is divisible by a leading term of another polynomial (i.e., $\bar{H}$ is the reduced Gröbner basis). ■

In other words, our result states that the specialization of the Gröbner basis works for this particular kind of ideal J, but in general the specialization is not the reduced Gröbner basis. In the case $n = 2$, we prove the following stronger result.

Theorem 7.1.3. *Let K be any field and let $F = (f_1(x,y), f_2(x,y)) \in \mathrm{Aut}(K[x,y])$. Then the reduced Gröbner bases of its face functions produce automorphisms, where the Gröbner bases are computed with respect to any "tag" monomial ordering $\succ$ such that $K[x,y] \succ K[s,t]$; i.e.,*

$$\mathrm{Gbasis}(s - f_1(0,y), t - f_2(0,y)) = \{g_1(s,t), y - g_2(s,t)\},$$
$$\mathrm{Gbasis}(s - f_1(x,0), t - f_2(x,0)) = \{h_1(s,t), x - h_2(s,t)\},$$

where $(g_1(s,t), g_2(s,t))$ and $(h_1(s,t), h_2(s,t))$ are elements of the group $\mathrm{Aut}(K[s,t])$.

Conversely, let $p(t), q(t) \in K[t]$ such that one of them is nonconstant and the reduced Gröbner basis G of the ideal $I = (p(t) - x, q(t) - y)$ with respect to an ordering $\succ$ such that $K[t] \succ K[x,y]$ is

$$G = \{f_1(x,y), t - f_2(x,y)\}.$$

Then (f_1, f_2) is an automorphism, $(p(t), q(t))$ are face functions of an automorphism (g_1, g_2) whose inverse is exactly (f_1, f_2), and in this case $K[p(t), q(t)] = K[t]$.

Proof. Let $P = (p_1(x,y), p_2(x,y))$ be the inverse of F. Since

$$(s - f_1(x,y), t - f_2(x,y)) = (x - p_1(s,t), y - p_2(s,t)),$$

substituting $x = 0$, we obtain that $\{(p_1(s,t), y - p_2(s,t))\}$ is a Gröbner basis of the ideal $(s - f_1(0,y), t - f_2(0,y))$ in $K[s,t,y]$ under any ordering that satisfies $K[y] \succ K[s,t]$. If $\{p_1(s,t), y - p_2(s,t)\}$ is already reduced, the uniqueness of the reduced Gröbner basis gives that

$$(g_1(s,t), g_2(s,t)) = (p_1(s,t), p_2(s,t)) \in \mathrm{Aut}(K[s,t]).$$

If there are further reductions, the only possibility is to reduce $p_2(s,t)$ modulo $p_1(s,t)$. We apply the algorithm for decomposing an automorphism into a product of elementary automorphisms (see Theorem 6.8.5, page 348 in [80]). It follows from this algorithm that the reduction

$$\{p_1(s,t), p_2(s,t)\} \to \{p_1(s,t), g_2(s,t)\}$$

gives an automorphism (p_1, g_2) of $K[s,t]$. Hence the reduced Gröbner basis of the ideal $(p_1(s,t), y - p_2(s,t))$ is $\{p_1(s,t), y - g_2(s,t)\}$ and again

$$(g_1(s,t), g_2(s,t)) = (p_1(s,t), g_2(s,t)) \in \mathrm{Aut}(K[s,t]).$$

Conversely, since

$$I = (p(t) - x, q(t) - y) = (f_1(x,y), t - f_2(x,y)),$$

there exist polynomials $u_i, v_i \in K[x,y,t]$, $i = 1,2$, such that

$$\begin{aligned} f_1(x,y) &= (p(t) - x)u_1(x,y,t) + (q(t) - y)u_2(x,y,t), \\ t - f_2(x,y) &= (p(t) - x)v_1(x,y,t) + (q(t) - y)v_2(x,y,t). \end{aligned}$$

Substituting $x = p(t)$, $y = q(t)$, we obtain

$$f_1(p(t), q(t)) = 0, \quad f_2(p(t), q(t)) = t.$$

By [13, Theorem 2.3.4], $\{f_1(x,y)\}$ is the Gröbner basis of the ideal of $K[x,y]$

$$I \cap K[x,y] = \{f(x,y) \in K[x,y] \mid f(p(t), q(t)) = 0\}.$$

On the other hand, at least one of the polynomials $p(t)$ and $q(t)$ essentially depends on t, and $I \cap K[x,y]$ is a principal ideal generated by an irreducible polynomial. Hence $f_1(x,y)$ is irreducible. By the Abhyankar–Moh theorem (see Theorem 6), there exists a polynomial $h(x,y) \in K[x,y]$ such that $F_1 = (f_1, f_2 + hf_1)$ is an automorphism of $K[x,y]$. Let $F_1^{-1} = (p_1(x,y), q_1(x,y))$ be the inverse of F_1. We have

$$(p_1(f_1, f_2), q_1(f_1, f_2)) = (x,y)$$

and

$$(p_1(0,t), q_1(0,t)) = (p(t), q(t)).$$

By Proposition 7.1.2, $\{f_1(x,y), t - f_2(x,y) - h(x,y)f_1(x,y)\}$ is a (nonreduced) Gröbner basis of the ideal $(p(t) - x, q(t) - y)$ under any ordering that satisfies $K[t] \succ K[x,y]$, and the reduced Gröbner basis under the same ordering is $\{f_1(x,y), t - f_2(x,y)\}$. Arguing as in the first part of the proof (i.e., applying again the algorithm for decomposing F_1 into a product of elementary automorphisms), we obtain that $F = (f_1, f_2)$ is also an automorphism with $F^{-1}(0,t) = (p(t), q(t))$. ∎

Example 7.1.4. Consider the Nagata automorphism $N = (n_1, n_2, n_3)$, where

$$\begin{aligned} n_1 &= x - 2y(zx + y^2) - z(zx + y^2)^2, \\ n_2 &= y + z(zx + y^2), \\ n_3 &= z. \end{aligned}$$

Using MAPLE 6.0, we have computed the reduced Gröbner bases of all its face functions; i.e., the reduced Gröbner basis of the ideals

$$I_x = (s - n_1(0,y,z), t - n_2(0,y,z), u - n_3(0,y,z)),$$
$$I_y = (s - n_1(x,0,z), t - n_2(x,0,z), u - n_3(x,0,z)),$$
$$I_z = (s - n_1(x,y,0), t - n_2(x,y,0), u - n_3(x,y,0)),$$

with respect to the lexicographic ordering $x > y > z > s > t > u$. We obtain that

$$\begin{aligned}
\text{Gbasis}(I_x) &= \{y-t+ut^2+u^2s, z-u, -s-2t^3-2tus+ut^4+2u^2t^2s+u^3s^2\} \\
&= \{y-(t-u(t^2+us)), z-u, -(s+2t(t^2+us)-u(t^2+us)^2)\}, \\
\text{Gbasis}(I_y) &= \{x-s-tus-t^3, z-u, -t+ut^2+u^2s\} \\
&= \{x-(s+t(t^2+us)), z-u, -(t-u(t^2+us))\}, \\
\text{Gbasis}(I_z) &= \{x-s-2t^3, y-t, u\} = \{x-(s+2t^3), y-t, u\}.
\end{aligned}$$

Hence, the Gröbner basis of I_x produces the inverse of the Nagata automorphism

$$N^{-1} = (x + 2y(zx + y^2) - z(zx + y^2)^2, y - z(zx + y^2), z).$$

The Gröbner basis of I_z produces the automorphism $(x+2y^3, y, z)$, but the Gröbner basis of I_y produces the endomorphism

$$(x + y(y^2 + xz), y - z(y^2 + xz), z),$$

which is *not* an automorphism because its Jacobian matrix is not invertible. Moreover, it is also very easy to check that the Gröbner bases above are independent of the "tag" ordering of the monomials $\succ$ such that $K[x,y,z] \succ K[s,t,u]$.

The example above shows that the case $n = 3$ differs from the case $n = 2$. One may suggest the following problem:

Question 7.1.5. Let K be a field and $F = (f_1, \ldots, f_n) \in T(n, K)$. Do the reduced Gröbner bases for any "tag" monomial ordering of its face functions give rise to automorphisms?

By Theorem 7.1.3, this question has a positive answer if $n = 2$. If $n > 3$, the answer is negative because M. Smith [370] showed that the Nagata automorphism is stably tame. If we extend it to $K[x,y,z,v]$, assuming that it acts identically on the new variable v, it becomes tame; i.e., (n_1, n_2, n_3, v) is a tame automorphism. The computations in $K[x,y,z,v]$ give the same result as in $K[x,y,z]$, and in this way the Nagata's automorphism gives a counterexample to our question for $n > 3$. The following example shows that the answer is negative also for $n = 3$. The automorphism we consider below was discovered by Freudenburg [136] and is an example of a tame automorphism with nonlinear base locus. There is a conjecture that all

such automorphisms are wild. So, although the automorphism from [136] is tame, it has some "wild" properties.

Example 7.1.6. Let K be a field of characteristic zero and let $L = (y, x, z)$, $A = (x, y, z + x^3 - y^2)$, and $B = (x, y + x^2, z + x^3 + (3/2)xy)$ be elements of $T(3, K)$. We consider the automorphism $F = A \circ L \circ B \circ L^{-1}$, the functional composition of the polynomial maps A, L, B, and L^{-1}, the inverse of L. Then, $F = (f_1, f_2, f_3)$ is an element of $T(3, K)$, where $f_1 = x + z^2$, $f_2 = y + z^3 + (3/2)xz$, and $f_3 = z + x^3 - y^2 - 3xyz + (1/4)z^2(3x^2 - 8yz)$.

We compute the reduced Gröbner bases of all its face functions; i.e., the reduced Gröbner bases of the ideals

$$\begin{aligned} I_x &= (s - f_1(0, y, z), t - f_2(0, y, z), u - f_3(0, y, z)), \\ I_y &= (s - f_1(x, 0, z), t - f_2(x, 0, z), u - f_3(x, 0, z)), \\ I_z &= (s - f_1(x, y, 0), t - f_2(x, y, 0), u - f_3(x, y, 0)), \end{aligned}$$

with respect to the lexicographic ordering $x > y > z > s > t > u$. We get that all Gröbner bases produce tame automorphisms and one of them is the inverse of F.

Now consider $F^{-1} = G = (g_1, g_2, g_3)$, the inverse of F, which is also in $T(3, K)$:

$$\begin{aligned} g_1 &= -x^6 + x - z^2 + 2zx^3 - 2zy^2 + 2x^3y^2 - y^4, \\ g_2 &= 1/2(-x^9 + 2y - 3xz + z^3 - 3z^2x^3 + 3z^2y^2 + 3zx^6 - 6x^3zy^2 + 3zy^4 \\ &\quad + 3x^4 + 3x^6y^2 - 3x^3y^4 - 3xy^2 + y^6), \\ g_3 &= z - x^3 + y^2. \end{aligned}$$

We also compute the reduced Gröbner bases of all its face functions; i.e., the reduced Gröbner bases of the ideals

$$\begin{aligned} I_x &= (s - g_1(0, y, z), t - g_2(0, y, z), u - g_3(0, y, z)), \\ I_y &= (s - g_1(x, 0, z), t - g_2(x, 0, z), u - g_3(x, 0, z)), \\ I_z &= (s - g_1(x, y, 0), t - g_2(x, y, 0), u - g_3(x, y, 0)), \end{aligned}$$

with respect to the same lexicographic ordering $x > y > z > s > t > u$. As a result, we obtain

$$\begin{aligned} \text{Gbasis}(I_x) &= \{-2t + 2y + u^3, -4u + 4z + 4t^2 - 4tu^3 + u^6, s + u^2\}, \\ \text{Gbasis}(I_y) &= \{-s + x - u^2, 3z - 3s^3 - 4t^2 - 2tu^3 - u^6 - 3u, 2t + 2u^3 + 3us\}, \\ \text{Gbasis}(I_z) &= \{-s + x - u^2, 2y - 2t - 2u^3 - 3us, \\ &\qquad 4u + 4s^3 + 3s^2u^2 - 4t^2 - 8tu^3 - 12tus\}. \end{aligned}$$

Again, it turns out that $\text{Gbasis}(I_z)$ gives F, the inverse of G. Besides, $\text{Gbasis}(I_x)$ produces an automorphism, but $\text{Gbasis}(I_y)$ does *not* correspond to an automorphism. However, if we change the "tag" monomial ordering (e.g., consider the lexicographic ordering $x > y > z > t > s > u$), the reduced Gröbner bases of I_x, I_y, or I_z produce tame automorphisms.

The example above indicates that the Gröbner bases of the face functions of a tame automorphism F with respect to a "tag" monomial ordering may produce tame automorphisms, but with the same "tag" monomial ordering, the inverse F^{-1} may not. It also suggests modifying slightly Question 7.1.5 for the case $n = 3$.

Conjecture 7.1.7. Let $F = (f_1, f_2, f_3) \in T(3, K)$; i.e., F is a tame automorphism. There exists at least one "tag" monomial ordering that satisfies the condition $K[x, y, z] \succ K[s, t, u]$ such that the reduced Gröbner bases of the face functions of F under this ordering produce automorphisms.

It is clear that the positive answer to Conjecture 7.1.7 implies that the Nagata automorphism is not tame. We have made a lot of experiments with tame automorphisms of $K[x, y, z]$ with different lengths of the decomposition into a product of affine and triangular automorphisms. In all the cases, we have obtained confirmations of the conjecture. The computations above also suggest studying the following problems:

Question 7.1.8. Let $F = (f_1, \ldots, f_n) \in \mathrm{Aut}(K[X])$. Fix a "tag" monomial ordering. Then:

(i) Does at least one of the reduced Gröbner bases of the face functions of F give the inverse of the automorphism F?

(ii) Does at least one of the reduced Gröbner bases of its face functions give an automorphism?

By taking any linear automorphism involving all variables in the image of every variable, we obtain a negative answer to Question 7.1.8 (i). Another nontrivial counterexample is the following automorphism from the book by Cohn [80]:

$$C = (x + y(xy - yz), y, z + y(xy - yz)).$$

We have checked that no reduced Gröbner bases of its face functions produce the inverse of C. Moreover, C is a tame automorphism; in fact, it is the composition of tame automorphisms $L \circ G \circ L$, where $L = (x, y, x - z) \in A(3, K)$ and $G = (x + zy^2, y, z) \in J(3, K)$.

Finally, Question 7.1.8 (ii) is still an open problem for $n > 2$.

7.2 Lifting the Nagata Automorphism

Let $K\langle X\rangle$ be the free associative algebra freely generated by the set $X = \{x_1, \ldots, x_n\}$. One may consider this algebra as the algebra of polynomials in n noncommuting variables. The notion of tame and wild automorphisms of $K\langle X\rangle$ is introduced as in the case of $K[X]$. Every automorphism of $K\langle X\rangle$ induces an automorphism of $K[X]$, and every tame automorphism of $K[X]$

can be obtained in this way (i.e., it can be lifted to an automorphism of $K\langle X\rangle$).

The result of Makar-Limanov [233] and Czerniakiewicz [86] states that every automorphism of $K\langle x, y\rangle$ is tame. Again, the answer is still unknown for $n > 2$. Therefore, if an automorphism of $K[X]$ can be lifted to an automorphism of $K\langle X\rangle$, it may be regarded "not wilder" than the corresponding automorphism of the free algebra.

Problem 7.2.1. Can every automorphism φ of $K[X]$ be lifted to an automorphism ψ of $K\langle X\rangle$? If φ fixes the variables $x_1, \ldots, x_m$, can the lifting ψ be chosen in such a way that it fixes the same variables in $K\langle X\rangle$ as φ does? Can the Nagata automorphism be lifted?

If an automorphism φ of $K[X]$ cannot be lifted to an automorphism of $K\langle X\rangle$, we may ask the question of "how far" φ can be lifted. The natural way to measure the "distance" is in the language of T-ideals.

Definition 7.2.2. An ideal of $K\langle X\rangle$ is called a T-ideal if it is invariant under all endomorphisms of $K\langle X\rangle$.

T-ideals of $K\langle X\rangle$ have important properties that make them very useful for applications to automorphisms.

Proposition 7.2.3.

(i) *For every T-ideal U of $K\langle X\rangle$, there exists an algebra R such that U coincides with the ideal $T(R)$ of all polynomial identities in n variables of R; i.e., $f(x_1, \ldots, x_n) \in U$ if and only if $f(r_1, \ldots, r_n) = 0$ for all $r_1, \ldots, r_n \in R$. The factor algebra $F(R) = K\langle X\rangle/T(R)$ is called the relatively free algebra of rank n in the variety of algebras generated by R.*

(ii) *Every automorphism of $K\langle X\rangle$ induces an automorphism of $K\langle X\rangle/U$.*

Problem 7.2.4. For a given automorphism φ of $K[X]$, find the T-ideals U with the property that φ can be lifted to $K\langle X\rangle/U$.

For a background on PI-algebras, see the book by Rowen [323]. The theorem of Amitsur that over an infinite field the ideals $T(M_m(K))$ of polynomial identities of the $m \times m$ matrix algebra $M_m(K)$ are the only prime T-ideals and the Razmyslov–Kemer–Braun theorem [310, 174, 59] on the nilpotence of the radical of a finitely generated PI-algebra give that, over infinite fields, for every T-ideal U there exist positive integers m and k such that

$$T(M_m(K)) \supseteq U \supseteq T^k(M_m(K)).$$

Since our goal is to see whether an automorphism of $K[X]$ can be lifted to an automorphism of $K\langle X\rangle$, it is natural to consider liftings to $K\langle X\rangle/T^k(M_m(K))$ only. The following statement shows that the difficult part of the lifting is to $K\langle X\rangle/T(M_m(K))$ and $K\langle X\rangle/T^2(M_m(K))$ only.

Proposition 7.2.5. *For $k>2$, every endomorphism of $K\langle X\rangle/T^k(M_m(K))$ that induces an automorphism of $K\langle X\rangle/T^2(M_m(K))$ is an automorphism.*

Proof. We repeat the argument from [101] for $K\langle X\rangle/C^k$, where C is the commutator ideal of $K\langle X\rangle$. Let $U = T(M_m(K))$, $A = K\langle X\rangle/U^k$. We use the same symbols (e.g., X, U, etc.) for the images of objects from $K\langle X\rangle$ in A. Let $\bar{A} = A/U^2$. If $\varphi \in \mathrm{End}(A)$ induces an automorphism on $\bar{A}$, then there exists an endomorphism ψ of A such that $\varphi \circ \psi$ and $\psi \circ \varphi$ both induce the identity map on $\bar{A}$. Therefore, it is sufficient to prove that every endomorphism θ of A that induces the identity map on $\bar{A}$ is an automorphism. Let

$$\theta(x_i) = x_i + f_i, \quad f_i \in U^2, \quad i = 1, \ldots, n.$$

Consider any element $g \in U^p$. Since $f_i \in U^2$, it is easy to see that $\theta(g) - g \in U^{p+1}$. Hence θ induces the identity map on the factors U^p/U^{p+1}, $p = 0, 1, \ldots, k-1$. Since $U^k = 0$ in A, A is isomorphic (as a vector space) to

$$\bar{A} \oplus U^2/U^3 \oplus \cdots \oplus U^{k-1}/U^k$$

and θ acts identically on all these factors. Hence θ is invertible (i.e., an automorphism). ■

Umirbaev has shown that every automorphism of $K[X]$ can be lifted to an automorphism of the "free metabelian" associative algebra. This is the algebra $K\langle X\rangle/C^2$, where $C = T(M_1(K)) = T(K)$ is the commutator ideal of $K\langle X\rangle$. Therefore it can also be lifted to $K\langle X\rangle/C^k$ for any $k > 2$. If the answer to Problem 7.2.1 is negative, we may ask a more precise version:

Problem 7.2.6. Can every automorphism φ of $K[X]$ be lifted to $\mathrm{Aut}(K\langle X\rangle)/T(M_m(K))$ and $\mathrm{Aut}(K\langle X\rangle)/T^2(M_m(K))$ for $m > 1$? If φ fixes $x_1, \ldots, x_m$, can the lifting be chosen with the same property? How far can the Nagata automorphism be lifted with and without fixing one of the variables?

The construction of M. Smith [370] showing that the Nagata automorphism is stably tame is as follows.

A derivation ∂ of $K[X]$ is called locally nilpotent if for any $f \in K[X]$ there exists a positive integer p such that $\partial^p(f) = 0$. The derivation ∂ is triangular if $\partial(x_i) = f(x_{i+1}, \ldots, x_n)$, $i = 1, \ldots, n$. For ∂ locally nilpotent (and if the characteristic of K is equal to 0), the map $\exp\partial\colon K[X] \to K[X]$ defined by

$$\exp\partial(f) = f + \frac{\partial}{1!}f + \frac{\partial^2}{2!}f + \ldots, \quad f \in K[X],$$

is an automorphism of $K[X]$. If $w \in K[X]$ is in the kernel of ∂, then $\Delta = w\partial$ is also a locally nilpotent derivation.

The Nagata automorphism is equal to $\exp\Delta$ for the locally nilpotent derivation $\Delta = w(x,y,z)\partial$, where ∂ is the derivation of $K[x,y,z]$ defined by

$$\partial(x) = -2y, \quad \partial(y) = z, \quad \partial(z) = 0,$$

and $w(x,y,z) = y^2+xz$ is from the kernel of ∂. We extend the action of ∂ to $K[x,y,z,v]$ by $\partial(v) = 0$. Then the automorphism $\exp(w\partial)$ of $K[x,y,z,v]$ acts identically on v and is tame because

$$\exp(w\partial) = \tau^{-1} \circ \exp^{-1}(v\partial) \circ \tau \circ \exp(v\partial),$$

where τ is the tame automorphism fixing x,y,z and $\tau(v) = v + w(x,y,z)$. Besides, $\exp(v\partial)$ is also tame and acts on x,y,z,v by

$$\exp(v\partial)(x) = x - 2vy - v^2z, \quad \exp(v\partial)(y) = y + vz,$$
$$\exp(t\partial)(z) = z, \quad \exp(v\partial)(v) = v.$$

Considering the same automorphisms of $K\langle x,y,z,v\rangle$, we see that $\exp(v\partial)$ is no longer an automorphism because v does not commute with the variables. But we replace $\exp(v\partial)$ with the tame automorphism θ of $K\langle x,y,z,v\rangle$ defined by

$$\theta(x) = x - 2vy - v^2z, \quad \theta(y) = y + vz, \quad \theta(z) = z, \quad \theta(v) = v.$$

Considering the automorphism $\tau = (x,y,z,v+w)$ of $K\langle x,y,z,v\rangle$ with $w = y^2+xz$, we obtain the automorphism $\psi = \tau^{-1}\circ\theta^{-1}\circ\tau\circ\theta$, which induces an automorphism φ of $K[x,y,z,v]$ acting as the Nagata automorphism on x,y,z and φ fixing v. Unfortunately, we are not able to restrict ψ to an automorphism of $K\langle x,y,z\rangle$ because the variable v is not fixed by ψ and the images of x and y involve v. For example, if $[a,b] = ab-ba$ denotes the commutator of a and b, then

$$\psi(v) = v + (v-w)[y,z] + [v-w,y]z - (v-w)[v-w,z]z.$$

Our problem would be solved if we were able to find an automorphism ρ of $K\langle x,y,z,v\rangle$ that induces the identity map on $K[x,y,z,v]$ and acts on v as ψ. Then $\rho^{-1}\circ\psi$ will also induce the Nagata automorphism and will fix v. Therefore, if we factorize $K\langle x,y,z,v\rangle$ modulo the ideal generated by v, we will obtain a lifting of the Nagata automorphism to an automorphism of $K\langle x,y,z\rangle$. Hence it is worth trying to find a better lifting for the Nagata automorphism to $\mathrm{Aut}(K\langle x,y,z,v\rangle)$.

We have succeeded in giving an explicit lifting of the Nagata automorphism to $K\langle x,y,z\rangle/C^2$ that still fixes z. We hope that this lifting will be useful for further attempts to lift the Nagata automorphism to an automorphism of $K\langle x,y,z\rangle$. We have followed the procedure from the proof of the result of Umirbaev [390].

We work in the free metabelian algebra $M(X) = K\langle X\rangle/C^2$. We fix two sets of variables $Y = \{y_1,\ldots,y_n\}$ and $Z = \{z_1,\ldots,z_n\}$ and consider the

polynomial algebra $K[Y \cup Z]$. Changing a little the notation of Umirbaev, we define formal partial derivatives $\partial/\partial x_i$ assuming that

$$\frac{\partial x_i}{\partial x_i} = 1, \quad \frac{\partial x_j}{\partial x_i} = 0, \quad j \neq i,$$

and, for a monomial $u = x_{i_1} \dots x_{i_m} \in M(X)$,

$$\frac{\partial u}{\partial x_i} = \sum_{k=1}^{m} y_{i_1} \dots y_{i_{k-1}} z_{i_{k+1}} \dots z_{i_m} \frac{\partial x_{i_k}}{\partial x_i}.$$

The Jacobian matrix of an endomorphism φ of $M(X)$ is

$$J(\varphi) = \left(\frac{\partial \varphi(x_j)}{\partial x_i} \right),$$

which is a matrix with entries from $K[Y \cup Z]$. One of the main results of [390] is that the Jacobian matrix $J(\varphi)$ is invertible (as a matrix with entries from $K[Y \cup Z]$) if and only if φ is an automorphism of $M(X)$. Clearly, the invertibility of $J(\varphi)$ is equivalent to $0 \neq \det(J(\varphi)) \in K$.

Proposition 7.2.7. *The following endomorphism σ of $K\langle x, y, z\rangle/C^2$ is an automorphism that induces the Nagata automorphism of $K[x, y, z]$*

$$\sigma(x) = x - (y^2 + xz)y - y(y^2 + xz) - (y^2 + xz)^2 z,$$
$$\sigma(y) = y + (y^2 + xz)z, \sigma(z) = z.$$

Proof. For simplicity of notation, we assume that

$$X = \{x, y, z\}, \quad Y = \{x_1, y_1, z_1\}, \quad Z = \{x_2, y_2, z_2\}.$$

Clearly, the endomorphism σ of $M(X)$ induces the Nagata automorphism of $K[X]$. In order to show that σ is an automorphism, it is sufficient to calculate the determinant of its Jacobian matrix. The partial derivatives of $\sigma(x)$, $\sigma(y)$, and $\sigma(z)$ are

$$\frac{\partial \sigma(x)}{\partial x} = 1 - (y_1 + y_2)z_2 - (y_1^2 + x_1 z_1 + y_2^2 + x_2 z_2)z_2^2,$$
$$\frac{\partial \sigma(x)}{\partial y} = -(y_1 + y_2)^2 - (1 + (y_1 + y_2)z_2)(y_1^2 + x_1 z_1 + y_2^2 + x_2 z_2),$$
$$\frac{\partial \sigma(y)}{\partial x} = z_2^2, \quad \frac{\partial \sigma(y)}{\partial y} = 1 + (y_1 + y_2)z_2,$$
$$\frac{\partial \sigma(z)}{\partial x} = \frac{\partial \sigma(z)}{\partial y} = 0, \quad \frac{\partial \sigma(z)}{\partial z} = 1.$$

Hence the Jacobian determinant $|J(\sigma)|$ is equal to

$$\begin{vmatrix} 1 - (y_1 + y_2)z_2 - uz_2^2 & z_2^2 \\ -(y_1 + y_2)^2 - (1 + (y_1 + y_2)z_2)u & 1 + (y_1 + y_2)z_2 \end{vmatrix} = 1,$$

where $u = y_1^2 + x_1 z_1 + y_2^2 + x_2 z_2$, and σ is an automorphism. ■

We sketch how, using the proof in [390], we have found the lifting of the Nagata automorphism. We hope that our considerations may be useful for attempts to lift other automorphisms suspected to be wild. Let $\nu = (f_1(X), f_2(X), z)$ be the Nagata automorphism, where

$$f_1(X) = x - 2(y^2 + xz)y - (y^2 + xz)^2 z, \quad f_2(X) = y + (y^2 + xz)z.$$

Tracing the proof in [390], we know that the ideals of $K[Y \cup Z]$ generated by

$$f_1(Y) - f_1(Z), \quad f_2(Y) - f_2(Z), \quad z_1 - z_2 \quad \text{and} \quad x_1 - x_2, \quad y_1 - y_2, \quad z_1 - z_2$$

coincide and there is an invertible matrix $R = (r_{ij}) \in K[Y \cup Z]$ such that

$$(f_1(Y) - f_1(Z), f_2(Y) - f_2(Z), z_1 - z_2) = (x_1 - x_2, y_1 - y_2, z_1 - z_2)R.$$

We do not know if there is an algorithm to find the matrix R, but nevertheless we have found one matrix with this property:

$$R = \begin{pmatrix} 1 - z_2(y_1 + y_2) - z_2^2 u & z_2^2 & 0 \\ -(y_1 + y_2)^2 - (1 + z_2(y_1 + y_2))u & 1 + z_2(y_1 + y_2) & 0 \\ -x_1(y_1 + y_2) - (y_1^2 + x_1 z_1)^2 - x_1 z_2 u & y_1^2 + x_1(z_1 + z_2) & 1 \end{pmatrix}.$$

The next step in the proof is to calculate the Jacobian matrix of any endomorphism φ of $M(X)$ that induces ν on $K[X]$ and to compute $R - J(\varphi)$. We start with

$$\varphi = (x - 2(y^2 + xz)y - (y^2 + xz)^2 z,\ y + (y^2 + xz)z, z),$$

$$R - J(\varphi) = \begin{pmatrix} z_2(y_2 - y_1) & 0 & 0 \\ x_1 z_1 - x_2 z_2 & 0 & 0 \\ x_1(y_2 - y_1) & 0 & 0 \end{pmatrix}.$$

Again, by the proof in [390], there exist elements w_1, w_2, w_3 from the commutator ideal of $M(X)$ such that their derivatives are exactly the columns of $R - J(\varphi)$. In our case

$$w_1 = [x, y]z + x[z, y] = xzy - yxz, \quad w_2 = w_3 = 0,$$

and one automorphism σ of $M(X)$ that lifts the Nagata automorphism is

$$\sigma = (\varphi(x) + w_1,\ \varphi(y) + w_2,\ \varphi(z) + w_3).$$

Starting with the automorphism σ, we can find a better lifting of the Nagata automorphism to an automorphism of $K\langle x, y, z, v\rangle$. Let $\theta^*, \tau \in \operatorname{Aut} K\langle x, y, z, v\rangle$, where

$$\theta^* = (x - vy - yv - v^2 z, y + vz, z, v),$$
$$\tau = (x, y, z, v + w), \quad w = y^2 + xz.$$

Concrete calculations show that

$$\psi^* = \tau^{-1} \circ (\theta^*)^{-1} \circ \tau \circ \theta^*$$

is also a lifting of the Nagata automorphism that fixes the variable v modulo the commutator ideal and

$$\psi^*(v) = v + (v - w)[y, z].$$

Again, the elements $\psi^*(x)$ and $\psi^*(y)$ depend on v; for example,

$$\psi^*(y) = y + wz + (v - w)[y, z]z.$$

Although the expression for $\psi^*(v)$ is simpler than that for $\psi(v)$ obtained above, we do not know how to fix the variable v in $K\langle x, y, z, v\rangle$.

Effective lifting of automorphisms of $K[X]$ to automorphisms of the free metabelian algebra $M(X)$ relies on a result of Artamonov [20] on ideals of polynomial algebras: If the ideals $(p_1, \ldots, p_k)$ and $(q_1, \ldots, q_k)$ of $K[X]$ coincide, then there exists an invertible $k \times k$ matrix R with entries from $K[X]$ such that the following matrix equality holds:

$$(p_1, \ldots, p_k) = (q_1, \ldots, q_k)R.$$

We expect that the following stronger version of the theorem of Artamonov holds.

Conjecture 7.2.8. Let $\{p_1, \ldots, p_k, x_1, \ldots, x_m\}$ and $\{q_1, \ldots, q_k, x_1, \ldots, x_m\}$ generate the same ideal of the polynomial algebra $K[X]$. Then there exists an invertible matrix $R \in M_{k+m}(K[X])$ such that

$$(p_1, \ldots, p_k, x_1, \ldots, x_m)R = (q_1, \ldots, q_k, x_1, \ldots, x_m)$$

and R has the block form

$$\begin{pmatrix} * & 0 \\ * & E \end{pmatrix},$$

where 0 is the $k \times m$ matrix with zero entries and E is the $m \times m$ identity matrix.

If Conjecture 7.2.8 is true, this would imply a stronger version of the theorem of Umirbaev [390], which we state as another conjecture.

Conjecture 7.2.9. Let C be the commutator ideal of $K\langle X\rangle$. Every automorphism of $K[X]$ fixing the variables $x_1, \ldots, x_m$ can be lifted to an automorphism of $K\langle X\rangle/C^2$ also fixing $x_1, \ldots, x_m$.

8

The Embedding Problem

Let $K[x_1, \ldots, x_n]$ be the polynomial algebra in n variables over a field K. Any collection of polynomials $p_1, \ldots, p_m$ from $K[x_1, \ldots, x_n]$ determines an algebraic variety $\{p_i = 0,\ i = 1, \ldots, m\}$ in the affine space K^n. We shall denote this algebraic variety by $V(p_1, \ldots, p_m)$.

We say that two algebraic varieties $V(p_1, \ldots, p_m)$ and $V(q_1, \ldots, q_k)$ are *isomorphic* if the algebras of residue classes $K[x_1, \ldots, x_n]/\langle p_1, \ldots, p_m \rangle$ and $K[x_1, \ldots, x_n]/\langle q_1, \ldots, q_k \rangle$ are isomorphic. Here $\langle p_1, \ldots, p_m \rangle$ denotes the ideal of $K[x_1, \ldots, x_n]$ generated by $p_1, \ldots, p_m$.

On the other hand, we say that two algebraic varieties (or, rather, embeddings of the same algebraic variety in K^n) are *equivalent* if there is an automorphism of K^n that takes one of them onto the other. If any two embeddings of an algebraic variety in K^n are equivalent, we say that this algebraic variety has a *unique embedding* in K^n.

In this chapter, we address the following general problem: Given two isomorphic algebraic varieties in affine space K^n, find out whether or not they are equivalent under an automorphism of K^n. We call this the Embedding problem. A special case of this problem is a well-known Embedding conjecture of Abhyankar and Sathaye:

Problem 8.0.1 (the Embedding conjecture). Let $p \in K[x_1, \ldots, x_n]$, $n \geq 2$. If the algebra $K[x_1, \ldots, x_n]/\langle p \rangle$ is isomorphic to $K[x_1, \ldots, x_{n-1}]$, then p is a coordinate; or, in geometric language: If a hypersurface V in $\mathbb{C}^n$ is isomorphic to the hyperplane $\{x_1 = 0\}$, then it is equivalent to it.

The Embedding conjecture is known to be true for $n = 2$ due to Abhyankar and Moh [10] and Suzuki [380], and it remains open for $n \geq 3$.

Here we mostly address a more general Embedding problem and, in particular, give numerous examples of algebraic varieties (mostly hypersurfaces) with inequivalent embeddings in K^n (see Section 8.2). In fact, we give a rather general recipe for constructing such examples by borrowing the idea of Tietze transformations from combinatorial group theory (see Section 1.3).

In Section 8.1 below, we consider plane curves and, in particular, give an algorithm for deciding whether two given *parametric* curves in $\mathbb{C}^2$ are equivalent under an automorphism of $\mathbb{C}^2$. Here we borrow another idea from combinatorial group theory, the "peak reduction" idea due to Whitehead (see Section 1.2).

8.1 Embeddings of Curves in the Plane

Let $K[x, y]$ be the polynomial algebra in two variables over a field K of characteristic 0. Here we contribute toward a classification of polynomials from $K[x, y]$ by proving the following:

Theorem 8.1.1. *Let* $p(x, y) = ax^n + by^m + \sum_{im+jn \le mn} c_{ij} x^i y^j$, $a, b, c_{ij} \in K$, $i, j > 0$, a, b *are not both zero, and* $q(x, y) = Ax^r + By^s + \sum_{is+jr \le rs} b_{ij} x^i y^j$, $A, B, b_{ij} \in K$, $i, j > 0$, A, B *are not both zero. Suppose that* m *does not divide* n, n *does not divide* m, s *does not divide* r, r *does not divide* s, *and* $\max(m, n) \neq \max(r, s)$. *Then there is no automorphism* $\alpha \in \mathrm{Aut}(K[x, y])$ *that takes* $p(x, y)$ *to* $q(x, y)$.

Polynomials of the form given in Theorem 8.1.1 can be considered "canonical models" for their automorphic images. Note that if, say, m divides n, then the degree of the polynomial $p(x, y)$ in the statement of Theorem 8.1.1 can be reduced by applying an automorphism of the form $(x \to x + \mu \cdot y^{m/n};\ y \to \lambda y)$ with $\mu, \lambda \in K$. However, there is no guarantee that the resulting polynomial will have the same form. This shows how subtle the situation is.

In some special cases though, we can handle those polynomials with m divisible by n or vice versa. This is possible, for example, if some fiber of a given polynomial admits a one-variable polynomial parametrization $x = u(t)$; $y = v(t)$:

Proposition 8.1.2. *Suppose the fibers* $\{p(x, y) = 0\}$, $\{q(x, y) = 0\}$ *of two polynomials* $p, q \in \mathbb{C}[x, y]$ *admit one-variable polynomial parametrizations. Then one can effectively find out (even without knowing the parametrizations) if there is an automorphism of* $\mathbb{C}[x, y]$ *that takes* p *to* q.

In particular, if some fiber of a given polynomial is an irreducible simply connected curve, then, by a well-known theorem of Zaidenberg and Lin [220], this fiber admits a one-variable polynomial parametrization. More precisely, they prove that (when $K = \mathbb{C}$) every polynomial like that has

a canonical model of the form $x^k - y^l$ with $(k,l) = 1$. Upon combining this with our method, we have the following:

Theorem 8.1.3. *Let $p(x,y) \in \mathbb{C}[x,y]$ be a polynomial whose fiber $\{p(x,y) = 0\}$ is an irreducible simply connected curve. Then some automorphism of $\mathbb{C}[x,y]$ takes $p(x,y)$ to $x^k - y^l$ with $(k,l) = 1$, and:*

(a) $\max(k,l) \leq \deg(p(x,y))$;

(b) *either k or l divides* $\deg(p(x,y))$;

(c) *the Newton polygon of $p(x,y)$ is either a triangle or a line segment; i.e., $p(x,y)$ is of the form $ax^n + by^m + \sum_{im+jn<mn} c_{ij}x^iy^j$, $m,n \geq 0$. If m does not divide n, n does not divide m, and $m,n \neq 0$, then $m = k$ or l, and $n = l$ or k, respectively. Otherwise, either $p(x,y)$ is linear or the "leading" part $ax^n + by^m + \sum_{im+jn=mn} c_{ij}x^iy^j$ is a proper power of some other polynomial.*

Thus, in many situations it is possible to rule out polynomials without irreducible simply connected fibers just by inspection. In any case, by Proposition 8.1.2, there is an effective procedure for deciding if a given polynomial fiber is irreducible and simply connected.

The next application of our method concerns embeddings of algebraic curves in the plane.

Theorem 8.1.4. *For any $k \geq 2$, there is an irreducible algebraic curve (with one place at infinity) that has at least k inequivalent embeddings in the plane $\mathbb{C}^2$.*

Our Theorem 8.1.4 says that there are arbitrarily (but finitely) many isomorphic algebraic curves in $\mathbb{C}^2$, all of which belong to different orbits under the action of the group $\mathrm{Aut}(\mathbb{C}^2)$. A particular example of a curve like that would be $y = x^{p_0} - y^{p_1p_2\cdots p_k}$, where $p_0, p_1, \ldots, p_k$ are distinct primes, $p_0 > p_1p_2 \cdot \cdots \cdot p_k$.

Note that by a result of Abhyankar and Singh [12] an irreducible curve with one point at infinity cannot have infinitely many inequivalent embeddings in $\mathbb{C}^2$. We do not know if, upon dropping the condition of having one point at infinity, one can find a polynomial fiber that has infinitely many inequivalent embeddings.

We also note that the first example of an irreducible algebraic curve with one place at infinity that has at least two inequivalent embeddings in $\mathbb{C}^2$ was claimed in [11].

Now we say a few words about our general method. It is a well-known result of Jung and van der Kulk that every automorphism of $K[x,y]$ is a product of elementary and linear automorphisms. The main difficulty in finding a canonical model for a given polynomial is to prove that one can find a sequence of elementary and linear automorphisms that would reduce the degree *at every step* until it is further irreducible by any elementary

automorphism. Then this last polynomial, whose degree is irreducible, will be a canonical model.

To arrange that, we use two principal ideas. First, we mimic elementary automorphisms of $K[x, y]$ by "elementary transformations" of $K[t] \times K[t]$. Second, we use Whitehead's idea of "peak reduction" (see Section 1.2) to arrange a sequence of elementary transformations of $K[t] \times K[t]$ so that the maximum degree would decrease at every step. This is described in Section 8.1.1 below.

While the "peak reduction" always works for elementary transformations of $K[t] \times K[t]$, the first part (mimicking elementary automorphisms of $K[x, y]$ by elementary transformations of $K[t] \times K[t]$) is where the difficulty is. We managed to do that for polynomials of the form given in Theorem 8.1.1 and also for polynomials $p(x, y)$ whose fiber $\{p(x, y) = 0\}$ admits a one-variable polynomial parametrization $x = u(t)$; $y = v(t)$ (i.e., this fiber is a rational curve with one place at infinity). The latter is used in proving Proposition 8.1.2 and Theorem 8.1.3. Those parametrizable fibers actually constitute the most tractable class of plane algebraic curves. It seemed plausible that every parametric curve would have a unique embedding in $\mathbb{C}^2$. However, the following example from [339] shows that this is actually not the case.

Example 8.1.5. Let C_1 be the curve given parametrically by $x(t) = t+t^4$, $y(t) = t^3$, and C_2 the curve given by $u(t) = t + t^4$, $v(t) = 3t^3 + t^6$. Then C_1 is isomorphic to C_2 because $K[t+t^4, t^3] = K[t+t^4, 3t^3+t^6]$. Note that $t^3 = \frac{2}{9}(v(t)^2 - 4u(t)^3 + \frac{3}{2}v(t))$.

However, the two curves are inequivalent. The curve C_1 can be presented as $p(x, y) = x^3 - y(1 + y)^3 = 0$, whereas C_2 has a presentation $q(x, y) = 16x^6 - 8x^3y^2 - 12x^3y + y^4 - 51x^3 + 3y^3 + 15y^2 + 9y = 0$.

It is easy to see that the degree of either of these two polynomials cannot be reduced by a single elementary automorphism. Therefore, C_1 is inequivalent to C_2 by a result of Wightwick [401].

8.1.1 Elementary automorphisms and peak reduction

It is a well-known result of Jung and van der Kulk that every automorphism of $K[x, y]$ is a product of elementary and linear automorphisms. We give here a somewhat more precise statement that can be found in [80, Theorem 6.8.5]:

Proposition 8.1.6. *Every automorphism of $K[x, y]$ is a product of linear automorphisms and automorphisms of the form $x \to x+f(y)$; $y \to y$. More precisely, if (g_1, g_2) is an automorphism of $K[x, y]$ such that $\deg(g_1) \geq \deg(g_2)$, say, then either (g_1, g_2) is a linear automorphism or there exists a unique $\mu \in K^*$ and a positive integer d such that $\deg(g_1 - \mu g_2^d) < \deg(g_1)$.*

Now we are going to consider the direct product $K[t] \times K[t]$ of two copies of the one-variable polynomial algebra over K and introduce the following elementary transformations (ET) that can be applied to elements of this algebra:

(ET1) $(u, v) \to (u + \mu \cdot v^k, v)$ for some $\mu \in K^*$; $k \geq 2$.

(ET2) $(u, v) \to (u, v + \mu \cdot u^k)$.

(ET3) a nondegenerate linear transformation $(u, v) \to (a_1 u + a_2 v,\ b_1 u + b_2 v)$; $a_1, a_2, b_1, b_2 \in K$.

One might notice that some of these transformations are redundant; e.g., (ET1) is a composition of the other ones. The reason behind that will be clear a little later.

We shall need the following:

Proposition 8.1.7. *For any pair $(u, v) \in K[t] \times K[t]$, there is a (perhaps empty) sequence of elementary transformations that takes (u, v) to some $(\hat{u}, \hat{v})$ such that:*

(i) *the maximum of the degrees of polynomials decreases* at every step *in this sequence;*

(ii) *the maximum of the degrees in $(\hat{u}, \hat{v})$ is irreducible by* any *sequence of elementary transformations.*

Comment to (i)*: if it happens that u and v have the same leading terms, then, perhaps by somewhat abusing the language, we say that the transformation $(u, v) \to (u - v, v)$ reduces the maximum of the degrees.*

Proof. We shall use the "peak reduction" method to prove this statement. This means the following. If at some point of a sequence of ET the maximum degree goes up (or remains unchanged) before eventually going down, then there must be a pair of *subsequent* ET in our sequence (a "peak") such that one of them increases the maximum degree (or leaves it unchanged) and then the other one decreases it. We are going to show that such a peak can always be reduced. In other words, *if the maximum degree can be decreased by a sequence of ET, then it can also be decreased by a single ET.* To prove that, we have to consider many different cases, but all of them are quite simple.

Let (u, v) be a pair of polynomials from $K[t] \times K[t]$ with, say, $\deg(u) \leq \deg(v)$, and let α_1 and α_2 be two subsequent ET applied to (u, v), as described in the previous paragraph. Consider several cases:

(1) $\alpha_1 \colon (u, v) \to (u + \mu \cdot v^k, v)$ for some $\mu \in K^*$; $k \geq 2$.
This α_1 strictly increases the maximum degree since $\deg(u) \leq \deg(v)$ by the assumption. Now we have two possibilities for α_2 since a linear ET cannot decrease the maximum degree.

(a) $\alpha_2\colon (u+\mu\cdot v^k, v) \to (u+\mu\cdot v^k,\ v+\lambda(u+\mu\cdot v^k)^m)$ for some $\lambda \in K^*$; $m \geq 2$. But this obviously *increases* the maximum degree, contrary to our assumption.

(b) $\alpha_2\colon (u+\mu\cdot v^k, v) \to (u+\mu\cdot v^k+\lambda\cdot v^m, v)$. If this α_2 decreases the maximum degree, then we should have $\mu\cdot v^k = -\lambda\cdot v^m$, in which case $\alpha_2 = \alpha_1^{-1}$, and the peak reduction is just cancelling out α_1 and α_2.

(2) $\alpha_1\colon (u,v) \to (u, v+\mu\cdot u^k)$ for some $\mu \in K^*$; $k \geq 2$.
If this α_1 increases the maximum degree, this can only happen when $\deg(v+\mu\cdot u^k) = \deg(u^k)$, in which case we argue exactly as in case (1). However, since $\deg(u) \leq \deg(v)$, it might happen that this α_1 does not change the maximum degree. Then we consider two possibilities for α_2:

(a) $\alpha_2\colon (u, v+\mu\cdot u^k) \to (u, v+\mu\cdot u^k+\lambda\cdot u^m)$. If this α_2 decreases the maximum degree, then we should have $m \geq k$. If $m = k$, then $\alpha_1\alpha_2$ is equal to a single ET. If $m > k$, then, in order for α_2 to decrease the maximum degree, we must have $\deg(v)$ divisible by $\deg(u)$, in which case α_2 alone would decrease the maximum degree of (u,v); i.e., we can get rid of α_1.

(b) $\alpha_2\colon (u, v+\mu\cdot u^k) \to (u+\lambda(v+\mu\cdot u^k)^m,\ v+\mu\cdot u^k)$. But this α_2 can only change the degree of the first polynomial in the pair, and this is not where the maximum degree was.

(3) α_1 is linear (i.e., $\alpha_1\colon (u,v) \to (a_1u+a_2v, b_1u+b_2v)$; $a_1, a_2, b_1, b_2 \in K$). Again, we have two possibilities for α_2.

(a) $\alpha_2\colon (a_1u+a_2v, b_1u+b_2v) \to (a_1u+a_2v, b_1u+b_2v+\mu(a_1u+a_2v)^k)$. If $k = 1$, then α_2 is linear and therefore does not change the maximum degree. If $k > 1$, then α_2 might decrease the maximum degree, but this can only happen if $a_2 = 0$, in which case we could decrease the maximum degree of (u,v) by a single ET of the type (ET2).

(b) The case where α_2 is of the type (ET1) is completely similar.

Thus, in any of the cases considered, if there is a "peak", then we can reduce the number of ET in the sequence. An obvious inductive argument completes the proof of Proposition 8.1.7. ■

8.1.2 A classification of parametric curves

To prove Theorem 8.1.1, it is clearly sufficient to prove the following:

Proposition 8.1.8. *Let* $p(x,y) = ax^n + by^m + \sum_{im+jn<mn} c_{ij}x^iy^j$, $a, b, c_{ij} \in K$, a, b *are not both zero. Suppose that* m *does not divide* n, *and* n *does not divide* m. *Then no automorphism* $\alpha \in \mathrm{Aut}(K[x,y])$ *can reduce the degree of* $p(x,y)$.

First, we need the following:

Lemma 8.1.9. *Let $p(x,y)$ be a polynomial of the form $ax^n + by^m + \sum_{im+jn\le mn} c_{ij}x^iy^j$, $c_{ij} \in K$. Then applying an elementary or linear automorphism β to $p(x,y)$ gives a polynomial of the same form except perhaps in the case where m divides n or n divides m, say, $m = kn$, and $\beta\colon x \to x + \mu \cdot y^k;\ y \to y$ for some $\mu \in K^*$.*

Proof. The statement is obvious for a linear automorphism, so suppose we have an elementary automorphism $\beta\colon x \to x + \mu \cdot y^k;\ y \to y$ for some $\mu \in K^*;\ k \ge 2$. Then

$$\beta(p(x,y)) = ax^n + \mu^n y^{kn} + by^m + \sum_{i=1}^{n-1} b_{ij}x^iy^{k(n-i)} + \sum_{im+jn\le mn} c_{ij}\left(x^i + \mu^i y^{ki+j} + \sum_{s=1}^{i-1} a_{ij}x^s y^{k(i-s)+j}\right). \quad (8.1)$$

Now we have to consider three cases:

(a) $kn < m$. We have to show that for every monomial x^iy^j in (8.1), one has $im + jn \le mn$. This is not obvious only for monomials of the form $x^sy^{k(i-s)+j}$. Compute

$$sm + (k(i-s)+j)n = sm + kn(i-s) + jn. \quad (8.2)$$

To see that the right-hand side of (8.2) does not exceed mn, note that $sm + kn(i-s) < sm + m(i-s) = mi$ since $kn < m$. Therefore, $sm + (k(i-s)+j)n < mi + nj \le mn$ by the assumption.

(b) $kn > m$. In this case, the "leading part" of $\beta(p(x,y))$ is $x^n + \mu^n y^{kn}$, so we have to show that, for every monomial x^iy^j in (8.1), one has $ikn + jn \le kn^2$. Again, we only have to show that for monomials of the form $x^sy^{k(i-s)+j}$

$$skn + (k(i-s)+j)n = kni + jn. \quad (8.3)$$

Since $mi + nj \le mn$, after multiplying both sides by $\frac{kn}{m}$, we get $kni + \frac{kn^2}{m}j \le kn^2$. Since $\frac{kn^2}{m} > n$ (recall that $kn > m$), this yields $kni + jn \le kn^2$. Comparing this to (8.3) completes the proof in this case.

(c) $kn = m$. The same argument as in the previous case works here unless $\beta\colon x \to x + \mu \cdot y^k;\ y \to y$ for some $\mu \in K^*$, which can cause cancellation of the leading y^m, thereby losing control.

■

Proof of Proposition 8.1.8. By way of contradiction, assume there is $\alpha \in \mathrm{Aut}(K[x,y])$ that takes $p(x,y)$ to some $q(x,y)$ of smaller degree. Put

into correspondence to the polynomial $p(x, y)$ a pair of its *face polynomials* $(p(t, 0), p(0, t)) \in K[t] \times K[t]$. Furthermore, put into correspondence to elementary (linear) automorphisms of $K[x, y]$ elementary (linear) transformations (ET) of $K[t] \times K[t]$ as described in the previous section. Then the sequence of ET that corresponds to the automorphism α takes $(p(t, 0), p(0, t))$ to some $(u, v) \in K[t] \times K[t]$. Consider two cases:

(1) In the sequence of elementary (linear) automorphisms of $K[x, y]$ that takes $p(x, y)$ to $q(x, y)$, we do not have a situation described in the proof of Lemma 8.1.9, case (c) (in which case we have, in particular, $(u, v) = (q(t, 0), q(0, t))$ or $(q(0, t), q(t, 0))$). In this case, by Lemma 8.1.9 and Proposition 8.1.7, there must be an ET that decreases the maximum of the degrees of the polynomials $(p(t, 0), p(0, t))$. However, given the hypotheses of Proposition 8.1.8, this is readily seen to be impossible.

(2) Otherwise, at some point in the sequence of elementary (linear) automorphisms of $K[x, y]$ that takes $p(x, y)$ to $q(x, y)$, we must have a situation described in the proof of Lemma 8.1.9, case (c). In other words, there is an initial fragment of our sequence that ends up with an elementary automorphism that decreases the degree. Among all sequences like that, we can choose one of minimal length. For this sequence, we have the corresponding sequence of ET applied to $(p(t, 0), p(0, t))$. Again, the last ET in this sequence decreases the maximum of the degrees in a pair of polynomials, in which case, by Proposition 8.1.7 (or rather by its proof), the length of the sequence of ET can be reduced. Then the length of the corresponding sequence of elementary (linear) automorphisms of $K[x, y]$ will be reduced, too, contrary to our choice.

This contradiction completes the proof of Proposition 8.1.8 and thereby of Theorem 8.1.1. ■

8.1.3 Embeddings of curves in the plane

Before we get to the proof of Proposition 8.1.2 and Theorem 8.1.3, we make a general remark. If a polynomial fiber $\{p(x, y) = 0\}$ admits a one-variable polynomial parametrization $x = u(t)$; $y = v(t)$, where $u(t), v(t)$ have zero constant terms, then, by a result of McKay and Wang [242], the polynomial $p^k(x, y)$, where $k = [\mathbb{C}(t) : \mathbb{C}(u(t), v(t))]$, equals the resultant $R(x, y) = \mathrm{Res}_t(u(t) - x, v(t) - y)$. Moreover, they prove [242, Theorem 5] that the highest homogeneous part of $p^k(x, y)$ is obtained the same way (i.e., as a resultant) from the highest homogeneous parts of $u(t)$ and $v(t)$. This implies, in particular, that the Newton polygon of $p(x, y)$ is either

a triangle or a line segment; i.e., $p(x,y)$ is of the form

$$ax^n + by^m + \sum_{im+jn<mn} c_{ij}x^i y^j; \quad m,n \geq 0 \tag{8.4}$$

(see [242, Corollary 6]). Furthermore, from the fact that $p(x,y)$ is the minimal polynomial for $u(t)$ and $v(t)$, it follows that, for example, $p(x+y^k,y)$ is the minimal polynomial for $u(t)-v^k(t)$ and $v(t)$. This establishes a correspondence between elementary (linear) automorphisms of $K[x,y]$ applied to $p(x,y)$ and elementary (linear) transformations (ET) of $K[t]\times K[t]$ applied to $(u(t),v(t))$. Theorem 5 of [242] implies that in any sequence of elementary (linear) automorphisms of $K[x,y]$ applied to $p(x,y)$, all polynomials have the form (8.4), and therefore, by our Lemma 8.1.9, the corresponding sequence of ET applied to $(u(t),v(t))$ can be arranged so that it decreases the maximum of the degrees in a pair of polynomials at every step.

Proof of Proposition 8.1.2. First we show that both p and q have "canonical models"; i.e., automorphic images whose degrees cannot be reduced by any automorphisms of $\mathbb{C}[x,y]$. Indeed, by the remark above, both polynomials are of the form (8.4). If m divides n or n divides m, then we can reduce the degree of the polynomial by applying an elementary automorphism. This elementary automorphism can be easily found: if, say, $kn=m$, then we apply the automorphism $\beta\colon x\to x+\mu\cdot y^k;\ y\to y$ (see (8.1)) with $\mu=\sqrt[n]{-b}$.

Continuing in this way, we arrive at a polynomial of the form (8.4), where m does not divide n, n does not divide m, and, say, $m<n$. The other polynomial can be reduced to the same form with the degrees m' and n', respectively. Again, we can assume that $m'<n'$. Now, if $n'\neq n$, we conclude (by Theorem 8.1.1) that there is no automorphism of $\mathbb{C}[x,y]$ that takes $p(x,y)$ to $q(x,y)$.

If $n'=n$, then an automorphism taking p to q exists if and only if a combination of a linear automorphism with some automorphism of the form $\{x\to x;\ y\to y+f(x)\}$, where $\deg(f)<m/n$, can take p to q.

To figure out if this is possible, we have to consider coefficients of the polynomial $f(x)$ as indeterminates and find out if the corresponding system of polynomial equations in those indeterminates (together with indeterminates that are the coefficients coming from the linear automorphism) has a solution over $\mathbb{C}$. To do that, we can apply a well-known algorithm that makes use of Gröbner bases (see, e.g., [13]).

This latter algorithm is pretty slow in general. However, there is one special case of Proposition 8.1.2 where we do not have to apply this algorithm at all. This happens when we want to find out if a given polynomial is *coordinate* (i.e., an automorphic image of x). In that case, if at some point we get a polynomial of the form (8.4), where m does not divide n and n does not divide m, then the polynomial is coordinate if and only if $\max(m,n)=1$; no further analysis is needed. ■

Proof of Theorem 8.1.3. By a result of Zaidenberg and Lin [220], some automorphism of $\mathbb{C}[x,y]$ takes $p(x,y)$ to $x^k - y^l$ with $(k,l) = 1$. The polynomial fiber $\{x^k - y^l = 0\}$ admits a one-variable polynomial parametrization $x = t^l; y = t^k$. Therefore, by the remark in the beginning of this section, the polynomial fiber $\{p(x,y) = 0\}$ admits a parametrization $x = u(t); y = v(t)$, and there is a sequence of ET that takes $(u(t), v(t))$ to (t^l, t^k) so that the maximum of the degrees in a pair of polynomials decreases at every step except perhaps several terminal steps that do not change the maximum degree. This immediately implies parts (a) and (c) of Theorem 8.1.3.

Then, take the last ET in the sequence that decreases the maximum degree; i.e., after applying this ET, we get a pair of polynomials whose degrees are $\{k,k\}$, $\{k,l\}$, or $\{l,l\}$. That means the preceding pair of polynomials in the sequence either has degrees $\{km,k\}$ or $\{l,ml\}$ for some $m \geq 2$. In any case, either k or l divides the maximum of the degrees in the preceding pair of polynomials and therefore also divides the degree of the corresponding two-variable polynomial. An obvious inductive argument completes the proof of part (b). ■

Now we get to the following proof:

Proof of Theorem 8.1.4. We have to exhibit k polynomials $f_1, \ldots, f_k$ from $\mathbb{C}[x,y]$ such that $\mathbb{C}[x,y]/\langle f_i \rangle \cong \mathbb{C}[x,y]/\langle f_1 \rangle$ for every $i = 1, \ldots, k$, but none of those polynomials can be taken to another by an automorphism of $\mathbb{C}[x,y]$ (here the symbol $\cong$ means "is isomorphic to").

A particular collection of such polynomials is as follows (it is modeled on the corresponding example in combinatorial group theory [241]):

$$
\begin{aligned}
f_1 &= y - x^{p_0} + y^{p_1 p_2 \cdots p_k}, \text{ where } p_0, p_1, \ldots, p_k \text{ are distinct primes,} \\
&\quad p_0 > p_1 p_2 \cdot \cdots \cdot p_k; \\
f_2 &= y - (x^{p_0} - y^{p_2 \cdots p_k})^{p_1}; \\
f_3 &= y - (x^{p_0} - y^{p_3 \cdots p_k})^{p_1 p_2}; \\
&\ldots \\
f_k &= y - (x^{p_0} - y^{p_k})^{p_1 p_2 \cdots p_{k-1}}.
\end{aligned}
$$

We are now going to show that the corresponding algebras of residue classes are isomorphic. It will be technically more convenient to write those algebras of residue classes as "algebras with relations"; i.e., for example, instead of $\mathbb{C}[x,y]/\langle f_1 \rangle$ we shall write $\langle x, y \mid f_1 = 0 \rangle$. Following is the chain of isomorphism-preserving transformations (similar to Tietze transformations in group theory — see Section 1.3) that establishes the isomorphism between $\langle x, y \mid f_1 = 0 \rangle$ and $\langle x, y \mid f_2 = 0 \rangle$:

$$
\begin{aligned}
&\langle x, y \mid y = x^{p_0} - y^{p_1 p_2 \cdots p_k} \rangle \cong \langle x, y, z \mid y = x^{p_0} - y^{p_1 p_2 \cdots p_k};\ z = y^{p_1} \rangle \\
&\quad \cong \langle x, y, z \mid y = x^{p_0} - z^{p_2 \cdots p_k};\ z = y^{p_1} \rangle \cong \langle x, z \mid z = (x^{p_0} - z^{p_2 \cdots p_k})^{p_1} \rangle \\
&\quad \cong \langle x, y \mid y = (x^{p_0} - y^{p_2 \cdots p_k})^{p_1} \rangle.
\end{aligned}
$$

In a similar way, one can establish the isomorphism between $\langle x, y \mid f_1 = 0\rangle$ and $\langle x, y \mid f_i = 0\rangle$ for every $i = 2, \ldots, k$.

Applying our Theorem 8.1.1 shows that none of the polynomials f_i can be taken to f_j, $j \neq i$, by an automorphism of $\mathbb{C}[x, y]$ (the restriction $p_0 > p_1 p_2 \cdot \cdots \cdot p_k$ ensures that the conditions of Theorem 8.1.1 are satisfied).

Finally, the fact that the curve $\{f_1 = 0\}$ (and hence any curve $\{f_i = 0\}$) is irreducible is obvious since f_1 is of the form $u(x) + v(y)$ for nonconstant polynomials u, v. ■

8.2 Embeddings of Hypersurfaces in Affine Space

In this section, we address two general problems:

(I) how to find out whether or not two given algebraic varieties are isomorphic;

(II) how to find out whether or not two given algebraic varieties are equivalent.

Both problems have received a lot of attention over the years. For a survey on problem (I), we refer to [415]. The most substantial contributions to problem (II) are [10, 11, 380, 220] for equivalence in $\mathbb{C}^2$ and [158, 166, 371] for equivalence in higher dimensions. In the latter three papers, it is shown that if the codimension of an algebraic variety V in $\mathbb{C}^n$ is sufficiently large, then V has a unique embedding in $\mathbb{C}^n$. Examples of nonuniquely embedded varieties in higher dimensions are given in [90] (for $n = 5$) and [170] and [415] (for $n \geq 3$).

In this section, we give a simple generic procedure for constructing examples of isomorphic but inequivalent varieties in any dimension. Furthermore, we give a very simple yet efficient criterion for distinguishing isomorphic but inequivalent *hypersurfaces*. This criterion allows us to show that isomorphic hypersurfaces that we construct are actually inequivalent even under any *holomorphic* automorphism of the ambient space $\mathbb{C}^n$.

We start by addressing problem (I). Our contribution to (I) is Theorem 8.2.1 below. Before we give the statement, we introduce three types of isomorphism-preserving "elementary" transformations that can be applied to an arbitrary algebra of residue classes $K[x_1, \ldots, x_n]/R$, where R is an ideal of $K[x_1, \ldots, x_n]$ and K an arbitrary ground field. These transformations are modeled on Tietze transformations in groups (see Section 1.3).

(P1) *Introducing a new variable*: Replace $K[x_1, \ldots, x_n]/R$ by $K[x_1, \ldots, x_n, y]/R + \langle y - p(x_1, \ldots, x_n)\rangle$, where $p(x_1, \ldots, x_n)$ is an arbitrary polynomial.

(P2) *Canceling a variable* (this is the converse of (P1)): If we have an algebra of residue classes of the form $K[x_1,\dots,x_n,y]/\langle p_1,\dots,p_m,q\rangle$, where q is of the form $y - p(x_1,\dots,x_n)$, and $p_1,\dots,p_m \in K[x_1,\dots,x_n]$, replace this by $K[x_1,\dots,x_n]/\langle p_1,\dots,p_m\rangle$.

(P3) *Renaming the variables*: Replace variables $(x_1,\dots,x_n)$ by $(x_{i_1},\dots,x_{i_n})$, where $i_1,\dots,i_n$ are arbitrary distinct indices, not necessarily the integers in $\{1,\dots,n\}$.

Then we have:

Theorem 8.2.1. *Two algebras $K[x_1,\dots,x_n]/\langle p_1,\dots,p_m\rangle$ and $K[x_1,\dots,x_n]/\langle q_1,\dots,q_k\rangle$ are isomorphic if and only if one can get from one of them to the other by a sequence of transformations (P1)–(P3).*

In particular, two algebraic varieties $V(p_1,\dots,p_m)$ and $V(q_1,\dots,q_k)$ in $\mathbb{C}^n$ are isomorphic if and only if one can get from the algebra $\mathbb{C}[x_1,\dots,x_n]/\langle p_1,\dots,p_m\rangle$ to the algebra $\mathbb{C}[x_1,\dots,x_n]/\langle q_1,\dots,q_k\rangle$ by a sequence of transformations (P1)–(P3).

This result alone does not solve problem (I) since it does not give a hint on how to choose the polynomials $p(x_1,\dots,x_n)$ in (P1). Still, the result is quite useful because, on the one hand, it yields invariants (necessary conditions of isomorphism) of algebraic varieties and, on the other hand, gives an easy, practical way of constructing "exotic" examples of isomorphic algebraic varieties, thus providing, in particular, potential examples of isomorphic but inequivalent varieties.

Theorem 8.2.1 also has the following interesting corollary, which says that, although isomorphic algebraic varieties may not be equivalent, they are always *stably equivalent* (the precise meaning of that is clear from the statement below). Moreover, isomorphic varieties turn out to be stably equivalent under a *tame* automorphism. Recall that we call an automorphism tame if it is a product of elementary and linear automorphisms, where elementary automorphisms are those that change only one variable.

Corollary 8.2.2 (see [166, 371]). *If two algebraic varieties $V(p_1,\dots,p_m)$ and $V(q_1,\dots,q_k)$ in $\mathbb{C}^n$ are isomorphic, then the varieties $V(p_1,\dots,p_m,x_{n+1},\dots,x_{2n})$ and $V(q_1,\dots,q_k,x_{n+1},\dots,x_{2n})$ in $\mathbb{C}^{2n}$ are equivalent under a tame automorphism of $\mathbb{C}^{2n}$.*

We now describe some invariants of isomorphic varieties that can be obtained based on Theorem 8.2.1. Given a variety $V = V(q_1,\dots,q_m)$ (in $\mathbb{C}^n$) that contains another variety $V' = V(r_1,\dots,r_s)$, consider the Jacobian matrix $J(q_1,\dots,q_m) = (\frac{\partial q_i}{\partial x_j})$, $1 \le i \le m$, $1 \le j \le n$. Then, consider the image of this matrix under the natural homomorphism from $\mathbb{C}[x_1,\dots,x_n]$ onto $\mathbb{C}[x_1,\dots,x_n]/\langle r_1,\dots,r_s\rangle$. We denote this image by $A_R(V)$ and call it the *Alexander matrix* of the variety $V = V(q_1,\dots,q_m)$ with respect to the ideal $R = \langle r_1,\dots,r_s\rangle$. This resembles the Alexander matrix of a finitely presented group, which plays an important role in algebraic topology —

see, e.g., [62] or [85]. Continuing this parallel with the classical Alexander matrix, we consider *elementary ideals* E_k, $k \geq 0$, of the Jacobian matrix $J(q_1, \ldots, q_m)$ defined as follows:

if $0 < n - k \leq m$,	then E_k is the ideal of $\mathbb{C}[x_1, \ldots, x_n]$ generated by all $(n-k) \times (n-k)$ minors of the matrix $J(q_1, \ldots, q_m)$;
if $n - k > m$,	then $E_k = 0$;
if $n - k \leq 0$,	then $E_k = \mathbb{C}[x_1, \ldots, x_n]$.

Denote by $\bar{E}_k$ the image of E_k in $\mathbb{C}[x_1, \ldots, x_n]/R$. Then Theorem 8.2.1 allows us to show that $\bar{E}_k$ are invariants of isomorphic algebraic varieties. More precisely:

Theorem 8.2.3. *Let V_1 and V_2 be two algebraic varieties in $\mathbb{C}^n$, both containing a variety $V(r_1, \ldots, r_m)$. Consider Jacobian matrices J_1 and J_2 of the varieties V_1 and V_2. Let $E_k^{(1)}$ and $E_k^{(2)}$ be elementary ideals of J_1 and J_2, respectively, defined as above, and let $R = \langle r_1, \ldots, r_m \rangle$. Then, if the varieties V_1 and V_2 are isomorphic, one has $E_k^{(1)} + R = E_k^{(2)} + R$, after possibly renaming the variables in $E_k^{(1)} + R$.*

In Section 8.2.1, we give examples of applying Theorem 8.2.3 to distinguishing nonisomorphic algebraic varieties. Note that the condition $E_k^{(1)} + R = E_k^{(2)} + R$ is always actually verifiable since checking if two ideals of a polynomial algebra are equal can be done by using the Gröbner basis algorithm (see [13]). As far as renaming the variables is concerned, there are only finitely many ways of doing it without changing the whole set of variables.

Then, we consider another application of Theorem 8.2.1 — to constructing isomorphic but inequivalent algebraic varieties. The most practical way of doing it is illustrated by the following

Example 8.2.4. Let $f(x, y, z)$ be any polynomial, and let $p(x, y, z) = x - f(x^k, y, z)$; $q(x, y, z) = x - f^k(x, y, z)$; $k \geq 1$. Then the varieties $V(p)$ and $V(q)$ are isomorphic.

Indeed, the algebra $K[x, y, z]/\langle p \rangle$ can be generated by $u = x^k$, y, and z since in this algebra we have $x = f(x^k, y, z)$. These new generators u, y, z are subject to the relation $u = f^k(u, y, z)$ (i.e., the minimal polynomial of u, y, and z in the algebra $K[x, y, z]/\langle p \rangle$ is $u - f^k(u, y, z)$). Therefore, the varieties $V(p)$ and $V(q)$ are isomorphic. (In Section 8.2.2, we give a more formal and rigorous proof of this fact based on our Theorem 8.2.1; what we have just given here is a somewhat informal, "fast" version of the same method.)

Now that we have a procedure for constructing nontrivial examples of isomorphic algebraic varieties, we need invariants of *equivalent* varieties. It appears that, in many situations, one can get away with very simple

invariants. From now on, we are going to concentrate on *hypersurfaces*; i.e., on varieties of the form $V(p)$.

It turns out that *the number of zeros of the gradient* $\operatorname{grad}(p)$ is a rather sharp invariant of equivalent hypersurfaces. (The fact that it *is* an invariant follows immediately from the "chain rule" for partial derivatives.) Note that this number is, in general, different from the number of singularities of a hypersurface since a point where the gradient vanishes may not belong to the hypersurface.

Whereas the number of singular points is an intrinsic characteristic of a hypersurface (i.e., it is invariant under an isomorphism), the number of zeros of the gradient is not, and therefore it can be used to distinguish isomorphic but inequivalent hypersurfaces. This can be illustrated by the following simple example:

Example 8.2.5. Let $p(x,y,z) = x+y+z-xyz$ and $q(x,y,z) = x+y^2+yz-xyz$. Then $\operatorname{grad}(p)$ has two zeros, whereas $\operatorname{grad}(q)$ vanishes nowhere. Therefore, the hypersurfaces $V(p)$ and $V(q)$ are inequivalent. The fact that they are isomorphic can be established by the same method that we used in Example 8.2.4. The algebra $K[x,y,z]/\langle p\rangle$ can be generated by $u = xy$, y, and z since in this algebra $x = xyz - y - z$. These new generators are subject to the relation $u = (uz - y - z)y = uyz - y^2 - yz$, whence the isomorphism.

This example can be generalized to the following proposition:

Proposition 8.2.6. *For any* $n \geq 3$, *the hypersurface* $x_1 + x_2 + \cdots + x_n - x_1x_2\ldots x_n = 0$ *has at least two embeddings in* $\mathbb{C}^n$ *inequivalent under any algebraic, or even just holomorphic, automorphism of* $\mathbb{C}^n$.

We emphasize this particular result because it contrasts sharply with a result of Jelonek [160] saying that the "n-cross" $x_1x_2\ldots x_n = 0$ has a unique embedding in $\mathbb{C}^n$ for any $n \geq 3$. Our Section 8.2.2 contains many other examples of isomorphic but inequivalent hypersurfaces.

The question of whether or not the number of zeros of the gradient can possibly be useful in approaching the Embedding conjecture 8.0.1 seems interesting in its own right:

Problem 8.2.7. If a hypersurface $V(p)$ in $\mathbb{C}^n$ is isomorphic to a coordinate hyperplane, is it true that $\operatorname{grad}(p)$ vanishes nowhere?

If the answer to this problem is negative, that would also give an example of a polynomial some of whose fibers are isomorphic to $V(x_1)$ and some not. Indeed, suppose $X_0 \in \mathbb{C}^n$ is a zero of the gradient of p, and let $p(X_0) = c$. Then the hypersurface $V(p-c)$ has a singular point and therefore cannot be isomorphic to $V(x_1)$.

There is no polynomial like that in $\mathbb{C}[x_1,x_2]$ — see [10], but for polynomials in more than two variables the situation is unknown.

We note that Kaliman [169] showed that if all fibers of a polynomial $p = p(x_1, x_2, x_3)$ are isomorphic to $\mathbb{C}^2$, then p is coordinate. This condition was relaxed in [171] to "the general fiber of p is isomorphic to $\mathbb{C}^{2}$".

8.2.1 Invariants of isomorphic varieties

We start with the following proof:

Proof of Theorem 8.2.1. Since the "if" part of the theorem is obvious, we proceed with the "only if" part.

We are going to show that if the algebras $K[X] = K[x_1, \ldots, x_n]/\langle p_1, \ldots, p_m\rangle$ and $K[x_1, \ldots, x_n]/\langle q_1, \ldots, q_k\rangle$ are isomorphic, then we can take them both to the same algebra by a sequence of transformations (P1)–(P3).

We denote the former algebra by $K[X]/R$ and the latter by $K[X]/S$, where R and S are ideals of $K[x_1, \ldots, x_n]$ generated by $p_1, \ldots, p_m$ and $q_1, \ldots, q_k$, respectively. Upon applying the transformation (P3), we may assume that the latter algebra is of the form $K[Y]/S$, where the set $Y = \{y_1, \ldots, y_n\}$ does not overlap with X.

Then, by repeatedly applying the transformation (P1), we can get

$$K[X]/R \cong K[X \cup Y]/R + \sum_{i=1}^{n} \langle y_i - u_i(x_1, \ldots, x_n)\rangle,$$

where u_i are polynomials constructed as follows. Since $K[X]/R$ is isomorphic to $K[Y]/S$, there is a mapping $\varphi\colon K[X]/R \to K[Y]/S$ such that $\mathrm{Ker}(\varphi) = 0 + R$, and

$$y_i + S = u_i(\varphi(x_1 + R), \ldots, \varphi(x_n + R)) + S = \varphi(u_i(x_1, \ldots, x_n) + R).$$

Denote the ideal $\sum_{i=1}^{n} \langle y_i - u_i(x_1, \ldots, x_n)\rangle$ by U. Now comes the crucial point: we are going to show that $S \subseteq R + U$.

Suppose we have an arbitrary polynomial $w(y_1, \ldots, y_n) \in S$. Then $w(y_1, \ldots, y_n) = w((y_1 - u_1) + u_1, \ldots, (y_n - u_n) + u_n) \equiv w(u_1, \ldots, u_n) \pmod{U}$. On the other hand, $\varphi(w(u_1, \ldots, u_n) + R) = w(y_1, \ldots, y_n) + S$ since $y_i + S = \varphi(u_i + R)$. Thus, $w(u_1, \ldots, u_n) + R \in \mathrm{Ker}(\varphi) = 0 + R$, and therefore $w(y_1, \ldots, y_n) \in R + U$.

Again, since $K[X]/R$ is isomorphic to $K[Y]/S$, there is another mapping (the inverse of φ) $\psi\colon K[Y]/S \to K[X]/R$ such that $\mathrm{Ker}(\psi) = 0 + S$;

$$x_i + R = v_i(\psi(y_1 + S), \ldots, \psi(y_n + S)) + R = \psi(v_i(y_1, \ldots, y_n) + S),$$

and, furthermore, $\psi(\varphi(x_i + R)) = x_i + R$, which implies

$$v_i(u_1, \ldots, u_n) \equiv x_i \pmod{R}.$$

Then we have $x_i - v_i(y_1, \ldots, y_n) = x_i - v_i((y_1 - u_1) + u_1, \ldots, (y_n - u_n) + u_n) \equiv x_i - v_i(u_1, \ldots, u_n) \pmod{U} \equiv x_i - x_i \pmod{R} \equiv 0 \pmod{R}$. Therefore, $x_i - v_i(y_1, \ldots, y_n) \in R + U$.

Thus, we have shown

$$R + U = R + S + U + \sum_{i=1}^{n} \langle x_i - v_i \rangle$$

and therefore that the algebra $K[X]/R$ can be taken to $K[X \cup Y]/R + S + U + \sum_{i=1}^{n} \langle x_i - v_i \rangle$ by a sequence of transformations (P1), (P3). By the symmetry, the algebra $K[Y]/S$ can be taken to the same algebra by a sequence of (P1), (P3), and this completes the proof. ■

Proof of Corollary 8.2.2 follows immediately from the proof of Theorem 8.2.1 since transformations of the type (P1) that we have used are actually tame automorphisms of $K[X \cup Y]$. ■

Proof of Theorem 8.2.3 basically goes along the same lines as the standard proof of invariance of Alexander ideals — see, e.g., [85]. Namely, our transformations (P1) and (P2) are analogous to Tietze transformations applied to group presentations, so that the invariance of $E_k + R$ can be established similarly.

However, there is one subtlety here. We have to show that $E_k + R$ does not depend on a particular choice of generators of the ideal $\langle q_1, \ldots, q_m \rangle$; i.e., that the ideals $E_k + R$ are well-defined. Suppose $\{u_1, \ldots, u_b\}$ is another generating set of $\langle q_1, \ldots, q_m \rangle$, and let $u_j = \sum_{i=1}^{m} q_i \cdot w_{ij}$, $1 \leq j \leq b$, where w_{ij} are some polynomials.

Add b zero rows to the Jacobian matrix $J(q_1, \ldots, q_m)$. This does not change any of the E_k, which can be easily seen from the definition. Enumerate those zero rows somehow, and add to the row number j the combination of other rows $\sum_{i=1}^{m} Q_i \cdot w_{ij}$, where by Q_i we denote the row of partial derivatives of the polynomial q_i. Again, this operation does not affect any of the E_k. Now, modulo the ideal $\langle q_1, \ldots, q_m \rangle$, the combination of rows above equals $\sum_{i=1}^{m} \partial(q_i \cdot w_{ij}) = \partial(u_j)$, where by $\partial(z)$ we denote the row of partial derivatives of z. By the symmetry, we can obtain exactly the same $(m+b) \times (m+b)$ matrix over $\mathbb{C}[x_1, \ldots, x_n]/\langle q_1, \ldots, q_m \rangle$ from the Jacobian matrix $J(u_1, \ldots, u_b)$ without changing any of the $E_k + R$. This completes the proof. ■

We now illustrate Theorem 8.2.3 by a couple of examples.

Example 8.2.8. Let $p = p(x, y) = x^2 + xy + y^3$; $V_1 = V(p)$, and $q = q(x, y) = x^2 + y^3$; $V_2 = V(q)$. Then $J(p) = \mathrm{grad}(p) = (2x + y, x + 3y^2)$; $J(q) = \mathrm{grad}(q) = (2x, 3y^2)$. Therefore, for the matrix $J(p)$, we have $E_0^{(1)} + R = \langle 2x + y, x + 3y^2, p \rangle = \langle x, y \rangle$ (here we choose $R = \langle p, q \rangle$). If we rename the variables in $E_0^{(1)}$ (by switching x and y), we shall get the same ideal $\langle x, y \rangle$.

On the other hand, for the matrix $J(q)$, we have $E_0^{(2)} + R = \langle 2x, 3y^2, p, q \rangle = \langle x, y^2 \rangle$. Thus, V_1 and V_2 are not isomorphic.

The point of the next example is to present a situation where our invariants can distinguish algebraic varieties with the same topology. (We are appealing to an intuitively clear fact that minor perturbations of coefficients of a polynomial do not change the topology of a general fiber). We also note that Makar-Limanov [235] has come up with another way to distinguish varieties with the same topology by using purely algebraic invariants.

Example 8.2.9. Let $p = p(x, y, z) = x + xyz + z^2$; $q_k = kx + xy$, $k \in \mathbb{C}$. By using our invariants, we can show that $V(p, q_k)$ and $V(p, q_m)$ are nonisomorphic algebraic curves in $\mathbb{C}^3$ if $k \neq m$.

Let $R = \langle p, q_k \rangle$. Then the ideal $E_2^{(1)} + R$ for the Jacobian matrix $J(p, q_k)$ has the following (reduced) Gröbner basis with respect to *deglex* term ordering (see [13]): $\{x, z^2, kz+yz\}$. The ideal $E_2^{(2)} + R$ for the Jacobian matrix $J(p, q_m)$ has the (reduced) Gröbner basis $\{x, z^2, mz + yz\}$ with respect to the same term ordering.

Since the reduced Gröbner basis with respect to a particular term ordering is unique, it follows that the ideal $E_2^{(2)} + R$ is different from $E_2^{(1)} + R$ if $k \neq m$ (obviously, renaming the variables cannot change this fact), whence we get nonisomorphism.

8.2.2 Inequivalent isomorphic varieties

In this section, we give various examples of inequivalent embeddings of hypersurfaces in $\mathbb{C}^n$. In all of these examples, we use the number of zeros of the gradient to establish inequivalence, as described in Section 8.2. Therefore, in each case, we actually establish a stronger type of inequivalence than just being inequivalent under any algebraic automorphism of $\mathbb{C}^n$. All examples here are those of isomorphic hypersurfaces in $\mathbb{C}^n$ inequivalent under any *holomorphic* (i.e., complex analytic) automorphism of $\mathbb{C}^n$. Also, in all of these examples, whenever we show that a given hypersurface $V(p)$ has inequivalent embeddings in $\mathbb{C}^n$, it will follow that $V(p)$ has inequivalent embeddings in $\mathbb{C}^m$ for any $m > n$ as well.

Finally, we note that, by the examples below, we try to illustrate all possible combinations of numbers of zeros of $\mathrm{grad}(p)$ and $\mathrm{grad}(q)$ for isomorphic hypersurfaces $V(p)$ and $V(q)$. That is, we have examples where $\mathrm{grad}(p)$ vanishes nowhere but $\mathrm{grad}(q)$ has infinitely many zeros, examples where both $\mathrm{grad}(p)$ and $\mathrm{grad}(q)$ have finitely many but different numbers of zeros, and so on.

We start with the proof of Proposition 8.2.6, but before we proceed, we give a rigorous proof of isomorphism claimed in Examples 8.2.4 and 8.2.5 in Section 8.2.

In Example 8.2.4, we start with the algebra $K[x, y, z]/\langle p \rangle$, where $p = p(x, y, z) = x - f(x^k, y, z)$. We are now going to give a sequence of el-

ementary transformations (P1)–(P3) that will bring us to the algebra $K[x,y,z]/\langle q\rangle$. It will be technically more convenient to write those algebras of residue classes as "algebras with relations"; i.e., for example, instead of $K[x,y,z]/\langle p\rangle$ we shall write $\langle x,y,z \mid p=0\rangle$. The symbol $\cong$ below means "is isomorphic to".

$$\begin{aligned}\langle x,y,z \mid x=f(x^k,y,z)\rangle &\cong \langle x,y,z,u \mid x=f(x^k,y,z),\ u=x^k\rangle\\ &=\langle x,y,z,u \mid x=f(u,y,z),\ u=x^k\rangle\\ &=\langle x,y,z,u \mid x=f(u,y,z),\ u=f^k(u,y,z)\rangle\\ &\cong \langle y,z,u \mid u=f^k(u,y,z)\rangle \cong \langle x,y,z \mid x=f^k(u,y,z)\rangle.\end{aligned}$$

For Example 8.2.5, the sequence of elementary transformations looks as follows:

$$\begin{aligned}\langle x,y,z \mid x=xyz-y-z\rangle &\cong \langle x,y,z,u \mid x=xyz-y-z,\ u=xy\rangle\\ &=\langle x,y,z,u \mid x=uz-y-z,\ u=xy\rangle \cong \langle y,z,u \mid u=(uz-y-z)y\rangle\\ &\cong \langle x,y,z \mid x=(xz-y-z)y\rangle=\langle x,y,z \mid x=xyz-y^2-yz\rangle.\end{aligned}$$

From now on, we are going to use a faster, slicker way of establishing isomorphism, as is done in Section 8.2. We are now ready for:

Proof of Proposition 8.2.6. Let $p=p(x_1,\dots,x_n)=x_1+x_2+\cdots+x_n-x_1x_2\dots x_n$. Then, since the algebra $\mathbb{C}[x_1,\dots,x_n]/\langle p\rangle$ can be generated by $x_1x_2\dots x_{n-1},x_2,\dots,x_n$, we have, as in Example 8.2.5, the hypersurface $V(p)$ isomorphic to $V(q)$, where $q=x_1-(x_1x_n-x_2-\cdots-x_n)x_2x_3\dots x_{n-1}=x_1+x_2^2x_3\dots x_n+x_2x_3^2\dots x_{n-1}+\cdots+x_2\dots x_n-x_1x_2\dots x_n$.

Now compute the gradients: $\operatorname{grad}(p)=(1-x_2\dots x_n,1-x_1x_3\dots x_n,\dots,1-x_1x_2\dots x_{n-1})$. This gradient has $(n-1)$ zeros since, for $\operatorname{grad}(p)=0$, one must have $x_1=x_2=\cdots=x_n$, and hence $x_1^{n-1}=1$.

On the other hand, $\operatorname{grad}(q)=(1-x_2\dots x_n,2x_2x_3\dots x_n+\cdots+x_3\dots x_{n-1}x_n-x_1x_3\dots x_n,\dots,x_2\dots x_{n-1}-x_1x_2\dots x_{n-1})$. We are going to show that this gradient never vanishes.

Indeed, from the first component, we see that none of the $x_2,\dots,x_n$ can be equal to 0. Then, from the last component, we get $x_1=1$. Now, if we divide each component except the first and the last ones by $x_3\dots x_{n-1}$, we shall get a homogeneous system of linear equations in $x_2,x_3,\dots,x_{n-1}$ (note that x_n will cancel out since $x_1=1$). The first equation is $2x_2+x_3+\cdots+x_{n-1}=0$, and other equations are obtained from it by repeatedly applying the cyclic permutation on variables. A system like that is easily seen to have only the trivial solution $x_2=x_3=\cdots=x_{n-1}=0$, and then the first component of $\operatorname{grad}(q)$ is not zero. ∎

One more example that seems to be worth emphasizing is that of the tom Dieck–Petrie hypersurface in $\mathbb{C}^n$, $n\geq 3$, determined by the polynomial

$p(x,y,z) = x^2z - y^3z^2 - 3y^2z + 2x - 3y - 1$ (see [97]). This hypersurface has several remarkable properties — see [168]. Here we prove:

Proposition 8.2.10. *Let $V(p)$ be the hypersurface in $\mathbb{C}^n$, $n \geq 3$, determined by $p(x,y,z) = x^2z - y^3z^2 - 3y^2z + 2x - 3y - 1$. Then there is a hypersurface $V(q)$ isomorphic to $V(p)$ but such that there exists neither an algebraic nor a holomorphic automorphism of $\mathbb{C}^n$ that takes $V(p)$ onto $V(q)$.*

We note that the part about an algebraic automorphism was established in [170] by using different, somewhat more complicated techniques.

Proof of Proposition 8.2.10. Let $p = p(x,y,z) = x^2z - y^3z^2 - 3y^2z + 2x - 3y - 1$. Since in the algebra $\mathbb{C}[x,y,z]/\langle p\rangle$ one has $x = \frac{1}{2}y^3z^2 + \frac{3}{2}y^2z - \frac{1}{2}x^2z + \frac{3}{2}y + \frac{1}{2}$, this algebra can be generated by x^2, y, z. Therefore, as in Example 8.2.4, the hypersurface $V(p)$ is isomorphic to $V(q)$, where $q = x - (\frac{1}{2}y^3z^2 + \frac{3}{2}y^2z - \frac{1}{2}xz + \frac{3}{2}y + \frac{1}{2})^2$.

Now compute the gradients: $\operatorname{grad}(p) = (2 + 2xz, -3 - 3y^2z^2 - 6yz, x^2 - 2y^3z - 3y^2)$. This gradient has infinitely many zeros since the common zero locus of the three components is the same as that of $(x - y, xz + 1)$.

On the other hand, $\operatorname{grad}(q) = (1 + z \cdot Q, -(\frac{3}{2}y^2z^2 + 3yz + \frac{3}{2})Q, -(y^3z + \frac{3}{2}y^2 - \frac{1}{2}x)Q)$, where $Q = Q(x,y,z) = (\frac{1}{2}y^3z^2 + \frac{3}{2}y^2z - \frac{1}{2}xz + \frac{3}{2}y + \frac{1}{2})$. This gradient never vanishes.

Indeed, the second component is $-\frac{3}{2}(yz+1)^2Q$. Since $Q \neq 0$ (otherwise, the first component would be 1), we get $yz = -1$. Now, from the last component, we get $x = y^2$. Plug this into the first component and get $z = 0$, which contradicts $yz = -1$. ∎

To construct similar examples in $\mathbb{C}^2$ is somewhat more difficult since there is "less room" there. However, we managed to do that as well.

Example 8.2.11. Let $p = p(x,y) = x^2 + y^2 - 1$. We claim that the curve $V(p)$ has at least two inequivalent embeddings in $\mathbb{C}^2$.

Since $x^2 + y^2 = (x + iy)(x - iy)$, where $i^2 = -1$, the algebra $\mathbb{C}[x,y]/\langle p\rangle$ is isomorphic to $\mathbb{C}[x,y]/\langle xy - 1\rangle$. In this latter algebra, one has $x = x^2y$, so that $\mathbb{C}[x,y]/\langle xy - 1\rangle$ can be generated by x^2, y. Therefore, the curve $V(p)$ is isomorphic to $V(q)$, where $q = x^2y - 1$.

Obviously, $\operatorname{grad}(p)$ vanishes only at the origin, whereas $\operatorname{grad}(q)$ has infinitely many zeros.

Example 8.2.12. Let $p = p(x,y) = x - x^2 - x^2y - 1$. Since in the algebra $\mathbb{C}[x,y]/\langle p\rangle$ one has $x = x^2 + x^2y + 1$, this algebra can be generated by x^2, y. Therefore, the curve $V(p)$ is isomorphic to $V(q)$, where $q = x - (1 + x + xy)^2$.

Clearly, $\operatorname{grad}(p) = (1 - 2x - 2xy, -x^2)$ vanishes nowhere, whereas $\operatorname{grad}(q) = (1 - 2(1 + y)(1 + x + xy), -2x(1 + x + xy)$ vanishes at the point $(0, -\frac{1}{2})$.

Example 8.2.13. Let $p = p(x, y) = x - y - x^2y - x^2y^2$. In the algebra $\mathbb{C}[x, y]/\langle p \rangle$, one has $x = y + x^2y + x^2y^2$, and hence this algebra can be generated by x^2y, y. Therefore, the curve $V(p)$ is isomorphic to $V(q)$, where $q = x - (x + y + xy)^2y$.

To find zeros of grad(p) and grad(q) is not so easy in this example, but constructing Gröbner bases for both ideals $\langle p_x, p_y \rangle$ and $\langle q_x, q_y \rangle$ facilitates the process. The Gröbner basis (with respect to the lexicographic term ordering with $y > x$) for $\langle p_x, p_y \rangle$ turns out to be $\{4y^3 + 6^2 + 2y + x + 2, 4y^4 + 8y^3 + 4y^2 + 2y + 1\}$, whereas for $\langle q_x, q_y \rangle$ it is $\{36y^2 + 24y + 8x + 27, 4y^3 + 4y^2 + 3y + 1\}$.

Now we see that grad(p) has four zeros, whereas grad(q) has three zeros.

8.3 The Embedding Conjecture for Free Associative Algebras

In this section, we show that a problem similar to the Embedding conjecture admits an easy solution if a free associative algebra is considered in place of a polynomial algebra.

Let $A_n = K\langle x_1, \ldots, x_n \rangle$ be a free associative algebra over a field K. For $u \in A_n$, let $\langle u \rangle$ denote the ideal of A_n generated by u. We are going to give examples of elements $u \in A_n$, $n \geq 3$, such that the factor algebra of A_n over the ideal $\langle u \rangle$ is isomorphic to A_{n-1}, and yet u is not a primitive element of A_n (i.e., it cannot be taken to x_1 by an automorphism of A_n).

Theorem 8.3.1. *Let $u = x_1 - (x_1^2 + x_2x_3)x_3$. Then, for any $n \geq 3$, the factor algebra $A_n/\langle u \rangle$ is isomorphic to A_{n-1}, but u is not a primitive element of A_n.*

This, combined with Makar-Limanov's "Freiheitssatz" [234], gives a negative answer to a question of G. Bergman [80, p. 336, Problem 6]:

Corollary 8.3.2. *Let K be a field of characteristic 0. Let $u = x_1 - (x_1^2 + x_2x_3)x_3$. Then, for any $n \geq 3$, the factor algebra $A_n/\langle u \rangle$ is isomorphic to A_{n-1}, but no automorphism of A_n takes the ideal $\langle u \rangle$ to $\langle x_1 \rangle$.*

We note that $u = x_1 - (x_1^2 + x_2x_3)x_3$ is just one of the many elements providing a negative answer to Bergman's question. Other examples include $u_{k,m} = x_1 - (x_1^k + x_2x_3^m)x_3^m$ for any $k \geq 2$, $m \geq 1$.

Proof of Theorem 8.3.1. First of all, u is not primitive since the Fox gradient of u (see Section 9.2.1) is $(1 - x_1x_3, -x_3^2, 0)$, which is not left unimodular.

Now we are going to show that the factor algebra $A_n/\langle u \rangle$ is isomorphic to A_{n-1}. It will be technically more convenient to write factor algebras as "algebras with relations"; i.e., for example, instead of $A_n/\langle u \rangle$ we shall write $\langle x_1, \ldots, x_n \mid u = 0 \rangle$. Following is the chain of isomorphism-preserving

transformations (similar to Tietze transformations in group theory — see Section 1.3) that establishes the isomorphism between $\langle x, y, z \mid x = (x^2 + yz)z\rangle$ and $\langle x, y, z \mid x = 0\rangle$:

$$\begin{aligned}
\langle x, y, z \mid x = (x^2 + yz)z\rangle &\cong \langle x, y, z, t \mid x = (x^2 + yz)z,\ t = x^2\rangle \\
&\cong \langle x, y, z, t \mid x = (t + yz)z,\ t = x^2\rangle \cong \langle y, z, t \mid t = ((t + yz)z)^2\rangle \\
&\cong \langle x, y, z \mid x = ((x + yz)z)^2\rangle \cong \langle x, y, z \mid x = (x + yz)z(x + yz)z\rangle \\
&\cong \langle x, y, z \mid x - yz = xzxz\rangle \cong \langle x, y, z \mid x = (xzx + y)z\rangle \\
&\cong \langle x, y, z \mid x = yz\rangle \cong \langle x, y, z \mid x = 0\rangle.
\end{aligned}$$

■

Proof of Corollary 8.3.2. Let $u = x_1 - (x_1^2 + x_2x_3)x_3 \in K\langle x_1, \ldots, x_n\rangle$, and suppose there is a primitive element $p \in \langle u\rangle$. Apply an automorphism φ that takes p to x. Then $x \in \langle \varphi(u)\rangle$. But $\varphi(u)$ depends on at least two variables because it is not primitive and irreducible; therefore, by the Freiheitssatz [234], every element of $\langle u\rangle$ depends on at least two variables, too. This contradiction completes the proof. ■

If $n = 2$ and the ground field has characteristic 0, the isomorphism of $A_2/\langle u\rangle$ to A_1 does imply that u is a primitive element of A_2:

Proposition 8.3.3. *Let K be a field of characteristic 0, and let $u \in K\langle x, y\rangle$. If the factor algebra $K\langle x, y\rangle/\langle u\rangle$ is isomorphic to $K\langle x\rangle$, then u is a primitive element of $K\langle x, y\rangle$.*

Proof. Let $u \in K\langle x, y\rangle$, and let $K\langle x, y\rangle/\langle u\rangle$ be isomorphic to $K\langle x, y\rangle/\langle x\rangle$. Let $u^a \in K[x, y]$ be the natural abelianization of u. Then $K[x, y]/\langle u^a\rangle$ is isomorphic to $K[x, y]/\langle x\rangle$. By Abhyankar and Moh's theorem (Theorem 6), u^a is a *coordinate* in $K[x, y]$, i.e., it can be taken to x by an automorphism of $K[x, y]$.

Since there is an isomorphism φ between $K\langle x, y\rangle/\langle u\rangle$ and $K\langle x, y\rangle/\langle x\rangle$, we see that every element of the commutator ideal of $K\langle x, y\rangle$ belongs to the ideal $\langle x\rangle$; otherwise, φ would not be one-to-one because $\varphi(xy - yx) \in \langle x\rangle$ for any φ. Therefore, the ideal $\langle u\rangle$ contains all elements whose abelianization is u^a. One of them must be primitive; then, as in the proof of Corollary 8.3.2, we conclude that u must be primitive by the Freiheitssatz [234]. ■

9
Coordinate Polynomials

Let $P_n = K[x_1, \ldots, x_n]$ be the polynomial algebra over a field K of characteristic 0. Recall that a polynomial $p \in P_n$ is *coordinate* if it can be included in a generating set of cardinality n of the algebra P_n.

The main question under consideration in this chapter is how to recognize coordinate polynomials. At the time of this writing, there is no algorithm known for recognizing coordinates in P_n if $n \geq 3$. On the other hand, there are several different algorithms that recognize coordinates in P_2; we describe one of them in the next section.

In the hope of getting at least some reasonable necessary conditions for a polynomial to be coordinate, we consider what we call the *outer rank* of a polynomial:

Definition 9.0.1. The outer rank of a polynomial $p \in K[x_1, \ldots, x_n]$ is the minimal number of generators x_i on which an automorphic image of p can depend.

It is clear that the outer rank of a coordinate polynomial equals 1. The converse is not true, but *irreducible* polynomials of outer rank 1 with zero constant term are obviously coordinates.

The question of actually finding the outer rank of a given element has been considered for various algebraic systems. The first significant result in this direction should be attributed to Whitehead: based on his powerful combinatorial technique, it is possible to find the outer rank of an element of a free group — see [227].

Mikhalev and Zolotykh [273] have come up with an important observation: the outer rank of an element of a free Lie algebra turns out to

be equal to the rank (i.e., to the minimal number of generators) of the right ideal of the enveloping free associative algebra generated by partial (noncommutative) Fox derivatives of this element.

A similar result has been proved by Umirbaev [391] for elements of a free group. More specifically, the outer rank of a free group element is equal to the rank of the right ideal of the free group ring generated by partial Fox derivatives of this element (see our Section 1.4). This result was independently obtained also by Bergman [47].

9.1 Coordinates of Two-Variable Polynomial Algebras

The results described above might tempt one to assume that also in the case of a polynomial algebra P_n the outer rank of a polynomial p equals the rank of the ideal of P_n generated by partial derivatives of p. This, however, is not the case, as the following example shows. Partial derivatives of the polynomial $p = x_1 + x_1^2 x_2$ generate the whole algebra P_2 as an ideal; therefore, they generate an ideal of rank 1 (i.e., a *principal* ideal). At the same time, it is easy to see that the outer rank of this polynomial equals 2.

The analysis of this example has led us to the following observation. In the course of constructing a Gröbner basis of a given ideal, one uses "reductions"; i.e., transformations of the following type (see [13, pp. 39–43]): given a pair (p, q) of polynomials, set $S(p,q) = \frac{L}{\text{l.t.}(p)} p - \frac{L}{\text{l.t.}(q)} q$, where $\text{l.t.}(p)$ is the *leading term* of p (i.e., the *leading monomial* together with its coefficient); $L = \text{l.c.m.}(\text{l.m.}(p), \text{l.m.}(q))$ (here, as usual, l.c.m. means the least common multiple, and $\text{l.m.}(p)$ denotes the leading monomial of p). In this book, we'll always consider what is called "deglex ordering" in [13] — where monomials are ordered first by total degree and then lexicographically with $x_1 > x_2 > \cdots > x_n$.

Now a crucial observation is as follows. These Gröbner reductions appear to be of two essentially different types:

(i) *regular*, or *elementary*, transformations. These are of the form $S(p,q) = \alpha \cdot p - r \cdot q$ or $S(p,q) = \alpha \cdot q - r \cdot p$ for some polynomial r and scalar $\alpha \in K^*$. This happens when the leading monomial of p is divisible by the leading monomial of q (or vice versa). The reason why we call these transformations *elementary* is that they can be written in the form $(p,q) \to (\alpha_1 p, \alpha_2 q) \cdot M$, where M is an *elementary matrix* (i.e., a matrix that (possibly) differs from the identity matrix by a single element outside the diagonal). In the case when we have more than two polynomials $(p_1, \ldots, p_k)$, we also can write $(p_1, \ldots, p_k) \to (\alpha_1 p_1, \ldots, \alpha_k p_k) \cdot M$, where M is a $k \times k$ elementary matrix; elementary reduction here is actually applied to a pair of polynomials (as usual) while the other ones are kept fixed. Sometimes, it is more convenient for us to get rid of the co-

efficients α_i and write $(p_1, \dots, p_k) \to (p_1, \dots, p_k) \cdot M$, where M belongs to the group $\mathrm{GE}_k(P_n)$ generated by all elementary *and* diagonal matrices from $\mathrm{GL}_k(P_n)$. It is known [379] that $\mathrm{GE}_k(P_n) = \mathrm{GL}_k(P_n)$ if $k \geq 3$, and $\mathrm{GE}_2(P_n) \neq \mathrm{GL}_2(P_n)$ if $n \geq 2$ — see [78].

(ii) *singular* transformations — these are nonregular ones.

It appears that the reason why the outer rank of the polynomial $p = x_1 + x_1^2 x_2$ above is greater than the rank of the ideal $I_{d(p)}$ of P_2 generated by partial derivatives of p is the *presence of singular transformations* in the corresponding reduction process.

We say that a polynomial $p \in P_n$ has *unimodular gradient* if $I_{d(p)} = P_n$ (in particular, the ideal $I_{d(p)}$ has rank 1 in this case). Note that if the ground field K is algebraically closed, this is equivalent to the gradient being nonvanishing.

Then we have:

Theorem 9.1.1. *Let a polynomial $p \in P_2$ have unimodular gradient. Then the outer rank of p equals 1 if and only if one can get from $(d_1(p), d_2(p))$ to $(1, 0)$ by using only elementary transformations or, in the matrix form: if and only if $(d_1(p), d_2(p)) \cdot M = (1, 0)$ for some matrix $M \in \mathrm{GE}_2(P_2)$.*

Our proof of Theorem 9.1.1 is based on a generalization of Wright's Weak Jacobian Theorem [404] — see Proposition 9.1.9.

Remark 9.1.2. Elementary transformations that reduce $(d_1(p), d_2(p))$ to $(1, 0)$ can actually be chosen to be Gröbner reductions (i.e., to decrease the maximum degree of monomials *at every step*) — we prove it based on a recent result of Park (see Proposition 9.1.10).

Now we show how one can apply this result to the study of coordinate polynomials. It is easy to show that a coordinate polynomial has a unimodular gradient, but the converse is not true. On the other hand, we have:

Proposition 9.1.3. *A polynomial $p \in P_n$ is coordinate if and only if it has outer rank* 1 and *a unimodular gradient.*

Combining this proposition with Theorem 9.1.1 yields the following:

Theorem 9.1.4. *A polynomial $p \in P_2$ is coordinate if and only if one can get from $(d_1(p), d_2(p))$ to $(1, 0)$ by using only elementary Gröbner reductions.*

This immediately yields an algorithm for detecting coordinate polynomials in P_2. Our algorithm is very simple and fast: it has quadratic growth with respect to the degree of a polynomial. When p is revealed to be a coordinate polynomial, the algorithm also gives a polynomial that completes p to a basis of P_2.

In the case where $K = \mathbb{C}$, an alternative, somewhat more complicated algorithm has been reported in [120]. It is not known whether or not there is an algorithm for detecting coordinate polynomials in P_n if $n \geq 3$.

Remark 9.1.5. For $n \geq 3$, Theorem 9.1.1 is no longer valid since in this case, by a result of Suslin [379], the group $\mathrm{GL}_n(P_n) = \mathrm{GE}_n(P_n)$ acts transitively on the set of all unimodular polynomial vectors of dimension n, yet there are polynomials with unimodular gradient but of the outer rank 2 — see the example above. The "only if" part, however, is valid for an arbitrary $n \geq 2$ — see Proposition 9.1.6. It is also easy to show that one always has $\mathrm{orank}\, p \geq \mathrm{rank}(I_{d(p)})$ — see Lemma 9.1.8.

Finally, we show that our method also yields an algorithm that, given a coordinate polynomial $p \in P_2$, finds a sequence of elementary automorphisms (i.e., automorphisms of the form $x_1 \to x_1 + f(x_2)$; $x_2 \to x_2$ together with linear automorphisms) that reduces p to x_1 — see Remark 9.1.11.

9.1.1 Proofs of main results

We start by fixing some notation. We write $\mathrm{orank}(p)$ for the outer rank of a polynomial $p \in P_n$, and $I_{d(p)}$ for the ideal of P_n generated by partial derivatives $d_1(p), \ldots, d_n(p)$ of p. Naturally, $d_k(p)$ denotes the partial derivative of p with respect to x_k. For an automorphism φ that takes x_i to p_i, $1 \leq i \leq n$, the Jacobian matrix is defined as follows: $J_\varphi = (d_j(p_i))_{1 \leq i,j \leq n}$.

We need the "chain rule": if $p = \varphi(q)$ for some endomorphism φ, then (in the matrix form)

$$(d_1(p), \ldots, d_n(p)) = (\varphi(d_1(q)), \ldots, \varphi(d_n(q))) \cdot J_\varphi, \tag{9.1}$$

where J_φ is the Jacobian matrix of φ. There is also a useful product rule for the Jacobian matrices:

$$J_{\varphi(\psi)} = \psi(J_\varphi) \cdot J_\psi. \tag{9.2}$$

Proof of Proposition 9.1.3.

(i) Suppose p is coordinate. Then $\mathrm{orank}(p) = 1$ since, by definition, there is an automorphism of P_n that takes p to x_1.

Now let $p = \varphi(x_1)$ for some automorphism φ. Then, applying the "chain rule" (9.1), we get

$$(d_1(p), \ldots, d_n(p)) = (\varphi(d_1(x_1)), \ldots, \varphi(d_n(x_1))) \cdot J_\varphi.$$

This gives

$$(d_1(p), \ldots, d_n(p)) = (1, 0, \ldots, 0) \cdot J_\varphi. \tag{9.3}$$

Since φ is an automorphism, the Jacobian matrix J_φ is invertible, so that (9.3) gives

$$(d_1(p), \ldots, d_n(p)) \cdot J_\varphi^{-1} = (1, 0, \ldots, 0),$$

implying $1 \in I_{d(p)}$, so $I_{d(p)} = P_n$.

(ii) Now suppose $\operatorname{orank}(p) = 1$ and $I_{d(p)} = P_n$. After applying an automorphism (if necessary), we can reduce p to the form $p = \sum_i \alpha_i x_1^i$, where $\alpha_i \in K$. Therefore, $d_1(p)$ should generate the whole P_n as an ideal. But this is only possible if $\alpha_i = 0$ for $i > 1$. Thus, p is coordinate. ■

Our next goal is to prove Theorem 9.1.1. First we prove the "only if" part of this theorem in a more general form:

Proposition 9.1.6. *Let $p \in P_n$ be a coordinate polynomial. Then one can get from $(d_1(p), \dots, d_n(p))$ to $(1, 0, \dots, 0)$ by using only elementary transformations.*

We need one lemma:

Lemma 9.1.7. *If φ is an automorphism of P_n, then the Jacobian matrix J_φ belongs to $\mathrm{GE}_n(P_n)$.*

Proof. The fact that J_φ belongs to $\mathrm{GL}_n(P_n)$ follows from the "chain rule". Now there are two cases:

(i) $n \geq 3$. Then we just have $\mathrm{GE}_n(P_n) = \mathrm{GL}_n(P_n)$ by a result of [379].

(ii) $n = 2$. In this case, the automorphism group of P_2 is generated by linear automorphisms together with automorphisms of the form $x_1 \to x_1 + f(x_2)$; $x_2 \to x_2$, where polynomial $f(x_2)$ does not depend on x_1 (see [164]). It is easy to see that the Jacobian matrix of any of those automorphisms belongs to $\mathrm{GE}_2(P_2)$; hence the Jacobian matrix of any automorphism of P_2 belongs to $\mathrm{GE}_2(P_2)$ as well — this follows from the product rule (9.2). ■

Now we are ready for the following proof:

Proof of Proposition 9.1.6. First of all, $I_{d(p)} = P_n$ by Proposition 9.1.3. Since p is coordinate, we have $p = \varphi(x_1)$ for some automorphism φ. Arguing as in the proof of Proposition 9.1.3, we get

$$(d_1(p), \dots, d_n(p)) \cdot J_\varphi^{-1} = (1, 0, \dots, 0). \tag{9.4}$$

Since $J_\varphi^{-1} \in \mathrm{GE}_n(P_n)$ by Lemma 9.1.7, (9.4) implies that one can get from $(d_1(p), \dots, d_n(p))$ to $(1, 0, \dots, 0)$ by using only elementary transformations. ■

Proof of Theorem 9.1.1. The "only if" part follows from Proposition 9.1.6, so we proceed with the "if" part.

Again, we need one general lemma:

Lemma 9.1.8. *For an arbitrary polynomial $p \in P_n$, one has* $\operatorname{orank}(p) \geq \operatorname{rank}(I_{d(p)})$.

Proof. Let $\operatorname{orank}(p) = k$. Then, upon applying an automorphism (if necessary), we can assume that p has the form $p = p(x_1, \dots, x_k)$. Note that the rank of $I_{d(p)}$ does not change under applying an automorphism to p —

this is clear from the "chain rule" (9.1). Now we see that the ideal $I_{d(p)}$ can be generated by k elements. ■

Back to the proof of Theorem 9.1.1, we see that by Lemma 9.1.8 the only case where we could possibly have $\operatorname{orank}(p) \neq \operatorname{rank}(I_{d(p)})$ is where $\operatorname{orank}(p) = 2$, whereas $\operatorname{rank}(I_{d(p)}) = 1$.

Since one can get from $(d_1(p), d_2(p))$ to $(1, 0)$ by using only elementary transformations, we have

$$(d_1(p), d_2(p)) \cdot M = (1, 0)$$

for some matrix $M \in \mathrm{GE}_2(P_2)$.

Let $M = \left(\begin{smallmatrix} q_1 & r_1 \\ q_2 & r_2 \end{smallmatrix}\right)$, so that

$$d_1(p)r_1 + d_2(p)r_2 = 0. \tag{9.5}$$

Since $M \in \mathrm{GL}_2(P_2)$, the column $\left(\begin{smallmatrix} r_1 \\ r_2 \end{smallmatrix}\right)$ must be unimodular; i.e., for some polynomials $s_1, s_2 \in P_2$, we have

$$s_1 r_1 + s_2 r_2 = 1.$$

This together with (9.5) gives

$$\begin{pmatrix} d_1(p) & d_2(p) \\ s_1 & s_2 \end{pmatrix} \cdot M = \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} = M_1.$$

The matrix M_1 belongs to $\mathrm{GE}_2(P_2)$ because it is triangular. Hence the matrix $J = \left(\begin{smallmatrix} d_1(p) & d_2(p) \\ s_1 & s_2 \end{smallmatrix}\right)$ belongs to $\mathrm{GE}_2(P_2)$, too.

Now we arrive at the most crucial point of the proof. We are going to use a result of [404] (Weak Jacobian Theorem) in a somewhat stronger form. The result itself says: if p, q are two polynomials from P_2, and the corresponding Jacobian matrix $J = \left(\begin{smallmatrix} d_1(p) & d_2(p) \\ d_1(q) & d_2(q) \end{smallmatrix}\right)$ belongs to $\mathrm{GE}_2(P_2)$, then p and q generate P_2; in particular, they both are coordinate polynomials.

A closer look at the (inductive) argument in the proof of this result (see [404, p. 250]) shows that the condition on the *second* row of the matrix J to have the form $(d_1(q)\ d_2(q))$ is not actually used. In other words, the result can be strengthened as follows:

Proposition 9.1.9. *If J is a matrix of the form $\left(\begin{smallmatrix} d_1(p) & d_2(p) \\ s_1 & s_2 \end{smallmatrix}\right)$, and $J \in \mathrm{GE}_2(P_2)$, then p is a coordinate polynomial.*

Proof of this proposition repeats the proof of Theorem 6 from [404] until "the very last moment", when the actual induction step is being done. Since we do not know a priori whether our matrix J is the Jacobian matrix of some endomorphism φ, we cannot talk about composing φ with the elementary automorphism ψ constructed in the course of the proof of Theorem 6 in [404, p. 250].

Instead, having in mind the product rule (9.2), we just consider the matrix $J^* = \psi(J) \cdot J_\psi$, where J_ψ is the Jacobian matrix of ψ and hence an elementary matrix. The same expansion of J^* as the one of $J_{\psi\varphi}$ in [404,

p. 250] shows that the "normal form" of J^* has smaller length than that of J. Hence we may refer to the inductive assumption as soon as we show that the first row of the matrix J^* still has the form $(\, d_1(q)\ d_2(q)\,)$ for some polynomial $q \in P_2$.

Indeed, it is straightforward to see that the first row of the matrix J^* is $(\, d_1(\psi(p))\ d_2(\psi(p))\,)$. This completes the proof of Proposition 9.1.9 and thereby the proof of Theorem 9.1.1 since we have shown that p is a coordinate polynomial, in particular $\operatorname{orank}(p) = 1$. ∎

Proof of Theorem 9.1.4. Our proof is based on the following result of H. Park [298] (we give it here in a little stronger form):

Proposition 9.1.10. *Let* $A = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{GE}_2(P_2)$ *and* $\mathrm{l.m.}(A) = \left(\begin{smallmatrix} \mathrm{l.m.}(p) & \mathrm{l.m.}(q) \\ \mathrm{l.m.}(r) & \mathrm{l.m.}(s) \end{smallmatrix}\right)$ *be the matrix of its leading monomials. Then, either at least three of the entries of* A *are constants or one of the rows of* $\mathrm{l.m.}(A)$ *is a monomial multiple of the other row and one of the columns is a monomial multiple of the other column.*

We give here a brief exposition of the proof.

The proof is by induction on the (minimum) number of elementary matrices E_i in a decomposition of the form

$$A = D \cdot E_1 \dots E_k, \quad k \geq 2,$$

where D is a diagonal matrix and $E_1 \dots E_k$ elementary matrices.

Since the matrix A is invertible, leading terms should cancel out when we compute the determinant of A; this means in the matrix $\mathrm{l.m.}(A)$ either all of the entries are constants, one of the entries is 0 and two of the others are constants, or $\det(\mathrm{l.m.}(A)) = 0$.

Let $\det(\mathrm{l.m.}(A)) = 0$. Denote $A' = D \cdot E_1 \dots E_{k-1}$, and consider two possibilities in accordance with our induction hypothesis.

(i) $\mathrm{l.m.}(A')$ has three constant entries. Let $E_k = \left(\begin{smallmatrix} 1 & 0 \\ g & 1 \end{smallmatrix}\right)$. There are three possibilities (up to a "symmetry") for the matrix $\mathrm{l.m.}(A')$:

(a) All the entries of $\mathrm{l.m.}(A')$ are constants. In this case, the matrix $\mathrm{l.m.}(A)$ is of the form $\left(\begin{smallmatrix} \mathrm{l.m.}(g) & 1 \\ \mathrm{l.m.}(g) & 1 \end{smallmatrix}\right)$. The result follows.

(b) Precisely three entries of $\mathrm{l.m.}(A')$ are constants. In this case, one of them is 0. Let $\mathrm{l.m.}(A') = \left(\begin{smallmatrix} f & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $\mathrm{l.m.}(A)$ has three constant entries.

(c) The same as (b), but $\mathrm{l.m.}(A') = \left(\begin{smallmatrix} 1 & f \\ 0 & 1 \end{smallmatrix}\right)$, f nonconstant. Then $\mathrm{l.m.}(A) = \left(\begin{smallmatrix} \mathrm{l.m.}(f) & \mathrm{l.m.}(g) & \mathrm{l.m.}(f) \\ \mathrm{l.m.}(g) & & 1 \end{smallmatrix}\right)$ so that the first row of $\mathrm{l.m.}(A)$ is $\mathrm{l.m.}(f)$ times the second row and the first column is $\mathrm{l.m.}(g)$ times the second column.

Now we come to the main case.

(ii) Let $A' = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and, say,

$$(\text{l. m.}(a), \text{l. m.}(b)) = h \cdot (\text{l. m.}(c), \text{l. m.}(d)); \tag{9.6}$$

$$(\text{l. m.}(a), \text{l. m.}(c)) = h' \cdot (\text{l. m.}(b), \text{l. m.}(d)) \tag{9.7}$$

for some nonconstant monomials h, h' (if some of them are constant, then we are done). This means, in particular, that a, b, c are nonconstant.

Again, we consider only one case here, where $E_k = \left(\begin{smallmatrix} 1 & g \\ 0 & 1 \end{smallmatrix}\right)$, $g \neq 0$. Then $A = \left(\begin{smallmatrix} a & b+ga \\ c & d+gc \end{smallmatrix}\right)$. Since $\det(A) = 1$, this yields

$$\text{l. m.}(c) \cdot \text{l. m.}(b + ga) = \text{l. m.}(a) \cdot \text{l. m.}(d + gc) = h \cdot \text{l. m.}(c) \cdot \text{l. m.}(d + gc).$$

Therefore, $\text{l. m.}(b + ga) = h \cdot \text{l. m.}(d + gc)$. This together with (9.6) means the first row of $\text{l. m.}(A)$ is h times the second row. Also, by (9.7), we have $\text{l. m.}(b + ga) = \text{l. m.}(ga) = \text{l. m.}(g) \cdot \text{l. m.}(a)$, and $\text{l. m.}(d + gc) = \text{l. m.}(gc) = \text{l. m.}(g) \cdot \text{l. m.}(c)$; hence the second column of $\text{l. m.}(A)$ is $\text{l. m.}(g)$ times the first column.

This completes the proof of Proposition 9.1.10.

To complete the proof of Theorem 9.1.4, we recall from the proof of Theorem 9.1.1 that polynomial p is coordinate if and only if the row $(d_1(p), d_2(p))$ can be completed to a matrix from $\mathrm{GE}_2(P_2)$. Combining this with Proposition 9.1.10 yields the result. ■

9.1.2 Algorithm for detecting coordinate polynomials

Given a polynomial $p = p(x_1, x_2)$, we want to figure out whether or not it is part of a basis of the polynomial algebra P_2.

Step 1. Take the derivatives $d_1(p)$, $d_2(p)$; denote $q_1 = d_1(p)$, $q_2 = d_2(p)$.

Step 2. If the leading monomial (l. m.) of q_1 is not divisible by the leading monomial of q_2 (or vice versa), then p is *not* part of a basis — this follows from Theorem 9.1.1 and Proposition 9.1.10. If $\text{l. m.}(q_1) = h \cdot \text{l. m.}(q_2)$ or $\text{l. m.}(q_2) = h \cdot \text{l. m.}(q_1)$ for some monomial h, then we go on to

Step 3. Set $q_1' = q_1 - h \cdot q_2$ or $q_2' = q_2 - h \cdot q_1$, respectively. If, say, $\text{l. m.}(q_1') = 1$, then p is part of a basis by Theorem 9.1.1. If $\text{l. m.}(q_1') = 0$, then p is part of a basis if and only if $\text{l. m.}(q_2) = 1$ (again by Theorem 9.1.1). If $\text{l. m.}(q_1') \neq 0$ or 1, then repeat Step 2 upon replacing q_1 with q_1' or q_2 with q_2', respectively.

Since the maximum of the degrees of q_1 and q_2 decreases every time we apply Step 3, we can apply it at most $d + (d-1) + \cdots + 1 = d(d+1)/2$ times, where d is the degree of the polynomial p. Therefore, our algorithm has quadratic growth with respect to the degree of a polynomial.

If our algorithm has revealed p to be a coordinate polynomial, then it is also easy to find a polynomial q such that p and q generate the whole algebra P_2. All we have to do is to keep track of the transformations in Step 3 in the matrix form as follows: $(q_1, q_2) \to (q_1, q_2)E(h)$, where $E(h) = \left(\begin{smallmatrix} 1 & 0 \\ -h & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & -h \\ 0 & 1 \end{smallmatrix}\right)$. In the end, if the polynomial p is coordinate, we arrive

at $(d_1(p), d_2(p)) = (1,0) \cdot M$, where M is a product of all the matrices $E(h)$ that we have encountered. It follows that M is of the form $\left(\begin{smallmatrix} d_1(p) & d_2(p) \\ s_1 & s_2 \end{smallmatrix}\right)$. Then, we conclude that $s_1 = d_1(q)$, $s_2 = d_2(q)$ for a polynomial $q \in P_2$, and p and q generate P_2.

Remark 9.1.11. This algorithm can also be used to find a sequence of elementary automorphisms that reduces $p \in P_2$ to x_1 in case p is a coordinate polynomial. Indeed, as we have just shown, we can find a matrix $M \in \mathrm{GE}_2(P_2)$ such that $(d_1(p), d_2(p)) = (1,0) \cdot M$ together with a decomposition of M into a product of elementary matrices. Then, applying the inductive argument from the proof of [404, Theorem 6] gives an effective procedure for constructing a desired sequence of elementary automorphisms.

Namely, suppose $M = E_{12}(p_1) \cdot E_{21}(q_1) \cdot \cdots \cdot E_{12}(p_k) \cdot E_{21}(q_k)$, where $E_{12}(p) = \left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right)$ and $E_{21}(q) = \left(\begin{smallmatrix} 1 & 0 \\ q & 1 \end{smallmatrix}\right)$. Then, from Wright's proof, it follows that $q_k = q_k(x_1)$ so that the matrix $E_{21}(q_k)$ is the Jacobian matrix of an elementary automorphism. Similarly, if the first elementary matrix on the right is of the form $E_{12}(p_k)$, then $p_k = p_k(x_2)$, whence $E_{12}(p_k)$ is the Jacobian matrix of an elementary automorphism. The inductive procedure now is clear.

Remark 9.1.12. An algorithm alternative to that of Remark 9.1.11 can be obtained as follows. Given a coordinate polynomial $p \in P_2$, we can find a polynomial q such that p and q generate P_2 — see above. Then we can use the procedure based on [80, Theorem 8.5] to reduce (p, q) to (x_1, x_2) by a sequence of elementary automorphisms. The difference between this algorithm and that of Remark 9.1.11 is (informally speaking) the same as between Nielsen's and Whitehead's algorithms in a free group (see Sections 1.1 and 1.2).

9.1.3 Relation to the Jacobian Conjecture

In this section, we discuss very briefly how our method may be used to construct a possible counterexample to the Jacobian conjecture in higher dimensions.

Proposition 9.1.13. *If polynomials $p_1, \ldots, p_n$ provide a counterexample to the Jacobian conjecture with minimal possible n, then each of those polynomials has outer rank bigger than* 1.

Proof. Suppose, say, p_1 has outer rank 1. Then, upon applying an automorphism (if necessary), we can assume that p_1 has the form $p_1 = p_1(x_1)$. In order to have the Jacobian matrix invertible, we should have then $p_1 = \alpha \cdot x_1$ for some $\alpha \in K^*$. Then, $(n-1) \times (n-1)$ Jacobian matrix $J' = (d_j(p_i))_{2 \le i,j \le n}$ is also invertible, which implies, by the minimality assumption, that $K(x_1)[p_2, \ldots, p_n] = K(x_1)[x_2, \ldots, x_n]$, where $K(x_1)$ is the quotient field of $K[x_1]$. It follows that $K(x_1, p_2, \ldots, p_n) = K(x_1, x_2, \ldots, x_n)$,

which by Keller's theorem [173] implies $K[x_1, p_2, \ldots, p_n] = P_n$. Therefore, polynomials $p_1, \ldots, p_n$ generate the whole algebra P_n and hence a contradiction. ■

This shows that polynomials with unimodular gradient, but of outer rank bigger than 1, are the key to constructing a counterexample to the Jacobian conjecture. By a result of Suslin [379], every unimodular polynomial row of dimension $n \geq 3$ can be completed to an invertible $n \times n$ matrix over P_n. Of course, the problem is to have those other $(n-1)$ rows satisfy the conditions $d_j(q_i) = d_i(q_j)$ for every row $(q_1, \ldots, q_n)$ — this is needed to make sure our invertible matrix is actually a Jacobian matrix.

The higher dimension of our unimodular row, the "more room" we have for building a matrix with the desired properties. There are several algorithms known for completing a unimodular polynomial row to an invertible square matrix over P_n (see, e.g., [224]), but all of them are rather complicated. A practical algorithm like that would be a major step toward constructing a counterexample to the Jacobian conjecture (if such a counterexample exists).

9.2 Coordinates in Free Associative Algebra of Rank Two

Here we use some results from the previous section to obtain information about automorphisms and coordinates of a free associative algebra of rank 2. We note that coordinates of a free associative algebra are usually called primitive elements (the same terminology is used in the theory of free groups).

Let $P_2 = K[x_1, x_2]$ be the polynomial algebra of rank 2 over a field K and $A_2 = K\langle x_1, x_2 \rangle$ the free associative algebra of rank 2 over the same ground field.

It is well-known that the automorphism groups $\mathrm{Aut}(P_2)$ and $\mathrm{Aut}(A_2)$ are isomorphic. This is due to Makar-Limanov [233] (for $K = \mathbb{C}$) and Czerniakiewicz [86] (for an arbitrary ground field). See also [80, Theorem 9.3].

Furthermore, there is a description of the group $\mathrm{Aut}(P_2)$ as a free product with amalgamation due to Shafarevich [334]; see also [80, Theorem 8.6], [94], [404], and references therein.

All these results, however, reduce a structure of the group $\mathrm{Aut}(P_2)$ to that of smaller groups of automorphisms. In this section, we show that a simple argument leads to a more specific group-theoretic description of $\mathrm{Aut}(P_2)$ (as well as of $\mathrm{Aut}(A_2)$). We only use the additive group of the ground field K as a "building block" and then apply various group-theoretic constructions.

We call an automorphism $\varphi \in \mathrm{Aut}(P_2)$ an *IL-automorphism* if it is identical on linear part (i.e., if it takes x_i to x_i+p_i, where polynomials p_i, $i = 1, 2$, don't have monomials of degree less than 2). A similar definition applies to automorphisms of A_2. Denote the groups of IL-automorphisms of P_2 and A_2 by $\mathrm{Aut}_{IL}(P_2)$ and $\mathrm{Aut}_{IL}(A_2)$, respectively. The subgroup $\mathrm{Aut}^e_{IL}(P_2)$ (or $\mathrm{Aut}^e_{IL}(A_2)$) is generated by *elementary* IL-automorphisms of the form $\{x_1 \to x_1 + f(x_2);\ x_2 \to x_2\}$ and $\{x_1 \to x_1;\ x_2 \to x_2 + f(x_1)\}$, where one-variable polynomials f don't have monomials of degree less than 2.

Furthermore, let $\mathrm{Aut}^\circ(P_2)$ (respectively, $\mathrm{Aut}^\circ(A_2)$) denote the group of *augmentation-preserving* automorphisms of P_2 (or A_2); these are automorphisms of the form $x_i \to x_i + p_i$, where polynomials p_i, $i = 1, 2$, have zero constant terms. Then we have:

Theorem 9.2.1. *Let K be an arbitrary ground field. The group $\mathrm{Aut}^\circ(A_2)$ is a semidirect product of $\mathrm{Aut}_{IL}(A_2)$ and $\mathrm{GL}_2(K)$ (the subgroup $\mathrm{Aut}_{IL}(A_2)$ being normal in $\mathrm{Aut}^\circ(A_2)$ and $\mathrm{GL}_2(K)$ a retract). The group $\mathrm{Aut}_{IL}(A_2)$ is the normal closure (in the group $\mathrm{Aut}^\circ(A_2)$) of $\mathrm{Aut}^e_{IL}(A_2)$. This latter group is isomorphic to the free product $(K^+)^\infty * (K^+)^\infty$, where $(K^+)^\infty$ is the direct sum of countably many copies of the additive group K^+ of the field K.*

All these statements remain valid upon replacing A_2 with P_2.

Thus, group-theoretic properties of the groups $\mathrm{Aut}^e_{IL}(P_2)$ and $\mathrm{Aut}^e_{IL}(A_2)$ (and these are the main building blocks of $\mathrm{Aut}(P_2)$ and $\mathrm{Aut}(A_2)$, respectively) are determined by properties of the additive group of the ground field K. This latter group may have a rather complicated structure, but in some cases (especially when K is finite), its structure is fairly well-understood.

Our further goal is to distinguish primitive elements of the algebra A_2 (an element $u \in A_2$ is called *primitive* if it is an automorphic image of x_1 or, in other words, if there is a generating set $\{u, v\}$ of A_2).

Based on the aforementioned isomorphism between $\mathrm{Aut}(P_2)$ and $\mathrm{Aut}(A_2)$, and also on results from the previous section on detecting generators of P_2, we can prove:

Theorem 9.2.2. *There is an algorithm that distinguishes primitive elements of the algebra A_2 over an arbitrary field of characteristic 0.*

Note that there is a very simple "commutator test" for deciding if a given *pair* of elements generates the algebra A_2 — see [93]. The problem of distinguishing primitive elements is obviously more difficult, yet our algorithm itself is fairly simple.

Furthermore, driven by the desire to reveal *nonprimitivity* of an element of A_2 just by inspection, we present a couple of very transparent *necessary* conditions for an element of A_2 to be primitive.

Denote by J_2 the *free special Jordan algebra* of rank 2. This is a (nonassociative) K-algebra spanned by x_1 and x_2 with respect to a binary operation

$x \circ y = \frac{1}{2}(xy + yx)$. To avoid a restriction $\operatorname{char} K \neq 2$, one can consider a somewhat less user-friendly definition of J_2 upon replacing the binary operation given above by two operations: $x \to x^2$ and $(x, y) \to xyx$.

Then we have:

Proposition 9.2.3. *For an arbitrary ground field K:*

(i) *The algebra J_2 is invariant under any automorphism of A_2.*

(ii) *The group* $\operatorname{Aut}(J_2)$ *is isomorphic to the group* $\operatorname{Aut}(A_2)$ *(and, consequently, to* $\operatorname{Aut}(P_2)$*).*

Corollary 9.2.4. *If $u \in A_2$ is a primitive element of A_2, then $u \in J_2$.*

This corollary gives a very convenient criterion for an element of A_2 to be primitive. Indeed, elements of J_2 are characterized among the elements of A_2 as follows (see [73] or [157]). Define an antiautomorphism $^{\leftarrow}$ of A_2 that rewrites every monomial backwards. For example, $(x_1x_2)^{\leftarrow} = x_2x_1$, $(x_1^2x_2x_1x_2^2)^{\leftarrow} = x_2^2x_1x_2x_1^2$, etc. Then $^{\leftarrow}$ is extended to the whole A_2 by linearity. The elements $u \in A_2$ for which $u^{\leftarrow} = u$ are called *palindromic.* Then we have [73] that an element $u \in A_2$ belongs to J_2 if and only if it is palindromic.

Thus our Corollary 9.2.4 gives a very convenient necessary (but not sufficient) condition of primitivity:

Corollary 9.2.5. *Primitive elements of A_2 are palindromic (which means, incidentally, that every* homogeneous component *of a primitive element is palindromic).*

This condition is quite sensitive since the algebra J_2 is very small compared to the enveloping algebra A_2.

We give here one more necessary condition of primitivity in A_2 based on a result of [350]. Denote by Δ the augmentation ideal of A_2 (i.e., the set of elements without constant terms). Every element $u \in \Delta$ has a unique presentation of the form $u = d_1(u) \cdot x_1 + d_2(u) \cdot x_2$ (see, e.g., [80]). The elements $d_i(u)$ are called (partial) Fox derivatives of u. Then we have:

Proposition 9.2.6. *If $u \in \Delta$ is a primitive element of A_2, then:*

$$(d_1(u))^{\leftarrow} \cdot d_2(u) = (d_2(u))^{\leftarrow} \cdot d_1(u).$$

In other words, the element $(d_1(u))^{\leftarrow} \cdot d_2(u)$ is palindromic.

This condition is also not sufficient for primitivity, but it seems plausible that, together with the condition of Corollary 9.2.4, it gives a sufficient condition for an element of the form $x_i +$ *(terms of higher degree)* to be primitive.

9.2.1 *Fox derivatives in a free associative algebra*

For an automorphism $\varphi \in \mathrm{Aut}(P_2)$ that takes x_i to p_i, $i = 1, 2$, the Jacobian matrix is defined as follows: $J_\varphi = (d_j(p_i))_{1 \le i,j \le 2}$, where d_j is the "usual" Leibniz partial derivation.

Similarly, if $\varphi \in \mathrm{Aut}(A_2)$ takes x_i to u_i, $i = 1, 2$, then $J_\varphi = (d_j(u_i))_{1 \le i,j \le 2}$, but this time d_j denotes partial Fox derivation. (We use the same notation for Leibniz and Fox derivations without ambiguity.)

There is a useful product rule for the Jacobian matrices (it is the same in commutative and noncommutative situations):

$$J_{\varphi(\psi)} = \psi(J_\varphi) \cdot J_\psi. \tag{9.8}$$

We are going to need some more background on Fox derivatives (the general reference here is [80]).

The augmentation ideal Δ of the algebra A_2 is a free left and right A_2-module with a free basis $\{x_i\}$, $1 \le i \le 2$, so that for any $u \in \Delta$ there is a unique presentation of the form $u = d_1(u) \cdot x_1 + d_2(u) \cdot x_2$ as well as of the form $u = x_1 \cdot D_1(u) + x_2 \cdot D_2(u)$. The elements $D_j(u)$ are called right Fox derivatives of u, and $d_j(u)$ are left Fox derivatives.

One can extend these derivations linearly to the whole A_2 by setting $D_i(1) = d_i(1) = 0$.

Then the result of [350] yields the following lemma:

Lemma 9.2.7. *Let u be a primitive element of A_2. Then $D_1(u) \cdot d_2(u) - D_2(u) \cdot d_1(u) = 0$.*

Proof. It has been proved in [350] that for an automorphism $\varphi \in \mathrm{Aut}(A_2)$ that takes x_i to y_i, $i = 1, 2$, one has

$$\begin{pmatrix} D_2(y_2) & -D_2(y_1) \\ -D_1(y_2) & D_1(y_1) \end{pmatrix} \cdot \begin{pmatrix} d_1(y_1) & d_2(y_1) \\ d_1(y_2) & d_2(y_2) \end{pmatrix} = c \cdot I,$$

where $c \in K^*$ and I is the identity matrix.

It follows (see, e.g., [80]) that

$$\begin{pmatrix} d_1(y_1) & d_2(y_1) \\ d_1(y_2) & d_2(y_2) \end{pmatrix} \cdot \begin{pmatrix} D_2(y_2) & -D_2(y_1) \\ -D_1(y_2) & D_1(y_1) \end{pmatrix} = c \cdot I,$$

whence $d_1(y_1) \cdot (-D_2(y_1)) + d_2(y_1) \cdot D_1(y_1) = 0$. This proves the claim. ■

We also need Nagao's theorem [287] (see also [404]):

Theorem 9.2.8 ([287]). $\mathrm{GL}_2(K[t]) = \mathrm{GL}_2(K) *_{\mathrm{UT}_2(K)} \mathrm{UT}_2(K[t])$, *where $K[t]$ is the polynomial algebra in one variable t over K, and UT_2 is a group of 2×2 upper triangular matrices. The statement is also valid upon replacing the upper triangular group with the lower triangular group.*

9.2.2 *Proofs and algorithms*

Proof of Theorem 9.2.1. We start with the first statement. It is straightforward to verify that $\mathrm{Aut}_{IL}(A_2)$ is a normal subgroup of $\mathrm{Aut}^\circ(A_2)$. Also, it is obvious that the intersection of $\mathrm{Aut}_{IL}(A_2)$ with the group of *linear* automorphisms is trivial. This means the group $\mathrm{Aut}^\circ(A_2)$ is a semidirect product of $\mathrm{Aut}_{IL}(A_2)$ and $\mathrm{GL}_2(K)$. (The fact that $\mathrm{Aut}^\circ(A_2)$ is a *product* of those two subgroups follows from the results of [86].)

It follows that every automorphism $\varphi \in \mathrm{Aut}^\circ(A_2)$ can be written in the form $\varphi = \lambda \circ \psi$, where λ is a linear automorphism, $\psi \in \mathrm{Aut}_{IL}(A_2)$, and $\lambda \circ \psi$ means $\lambda(\psi)$.

On the other hand, by the results of [86], every automorphism $\varphi \in \mathrm{Aut}^\circ(A_2)$ can be written as a product of linear automorphisms and elementary automorphisms of the form $\{x_1 \to x_1 + c \cdot x_2^m;\ x_2 \to x_2\}$ and $\{x_1 \to x_1;\ x_2 \to x_2 + c \cdot x_1^m\}$ for all possible $c \in K$ and $m \geq 2$. These elementary automorphisms clearly belong to the group $\mathrm{Aut}^e_{IL}(A_2)$. Now a usual rewriting process (based on the equality $abc = b(b^{-1}ab)c = ba^bc$) in combination with what was said in the previous paragraph proves the second statement of Theorem 9.2.1.

Now we are going to prove the claim about the group $G = \mathrm{Aut}^e_{IL}(A_2)$.

Denote two copies of $(K^+)^\infty$ by A and B and their natural components by $\{A_2, A_3, \dots\}$ and $\{B_2, B_3, \dots\}$, respectively (we deliberately start with index 2 for subsequent notational convenience). All the groups A_k and B_k are isomorphic to the group K^+.

We are now going to define a mapping τ from $A * B$ into G on these components; the fact that a mapping like that can be extended to a homomorphism of groups follows from categoric properties of the group-theoretic constructions involved.

Let τ take $a_i \in A_i$ to the following automorphism $\alpha_i\colon x_1 \to x_1 + a_i \cdot x_2^i$; $x_2 \to x_2$. Then, let τ take $b_i \in B_i$ to the automorphism $\beta_i\colon\ x_1 \to x_1$; $x_2 \to x_2 + b_i \cdot x_1^i$. Everywhere, $i \geq 2$.

First we prove that τ is injective. By way of contradiction, suppose, say, $\hat{\alpha}_1 \cdot \hat{\beta}_1 \cdot \dots \cdot \hat{\alpha}_k \cdot \hat{\beta}_k = \mathrm{id}$, where $\hat{\alpha}_i$ (or $\hat{\beta}_i$) is a product of finitely many α_{i_j} (or β_{i_j}), and id is the identical mapping. We assume that all $\hat{\alpha}_i$, $\hat{\beta}_i$ are nonidentical mappings.

Then applying the product rule (9.8) for the Jacobian matrices yields

$$\psi_1(J_{\hat{\alpha}_1}) \cdot \psi_2(J_{\hat{\beta}_1}) \cdot \dots \cdot \psi_k(J_{\hat{\alpha}_k}) \cdot J_{\hat{\beta}_k} = I, \tag{9.9}$$

where $\psi_j \in \mathrm{Aut}^e_{IL}(A_2)$ are appropriate automorphisms (of no particular importance to us), and I is the identity matrix.

All matrices $\psi_j(J_{\hat{\alpha}_i})$ are obviously upper triangular, and matrices $\psi_j(J_{\hat{\beta}_i})$ are lower triangular. Furthermore, none of them is the identity matrix, and, moreover, none of them belongs to the group $\mathrm{UT}_2(K)$ since none of the $J_{\hat{\alpha}_i}$, $J_{\hat{\beta}_i}$ do.

Consider now the abelianization $x_1 \to t$; $x_2 \to t$. An abelianized matrix $\psi_j(J_{\hat{\alpha}_i})^a$ or $\psi_j(J_{\hat{\beta}_i})^a$ doesn't belong to $\mathrm{UT}_2(K)$ unless it is the identity matrix.

Indeed, any off-diagonal entry in a matrix $\psi_j(J_{\hat{\alpha}_i})$, say, has the form $\psi_j(f(x_2))$, where f is some (nonconstant) one-variable polynomial, so that $\psi_j(f(x_2))^a = f(\psi_j(x_2)^a) \notin K$ since $\psi_j(x_2)$ must be either nonconstant or zero, so its abelianization is either nonconstant or zero, too.

Applying Nagao's theorem (see Theorem 9.2.8) to the abelianized equality (9.9) yields a contradiction (note that $J_{\hat{\beta}_k} \neq I$ in (9.9)) that completes the proof of τ being injective.

The fact that τ is surjective follows from the very definition of the group $\mathrm{Aut}^e_{IL}(A_2)$. Thus, τ is an isomorphism.

The corresponding statements about automorphisms of P_2 can now be easily deduced from the fact that the groups $\mathrm{Aut}^\circ(P_2)$ and $\mathrm{Aut}^\circ(A_2)$ are naturally isomorphic. We omit the details. ■

Proof of Theorem 9.2.2. Let $u \in A_2$. Denote by $u^a \in P_2$ the abelianization of u. If u^a is *not* a coordinate polynomial of P_2, then u is obviously not a primitive element of A_2. Note that we can decide whether or not u^a is coordinate using the algorithm from Section 9.1.2.

Let u^a be a coordinate polynomial of P_2. Using again a procedure from Section 9.1.2, we can find a sequence of elementary automorphisms that takes x_1 to u^a. Apply the same sequence to x_1 but in the algebra A_2 (we identify elementary automorphisms of P_2 and A_2 by means of the natural isomorphism mentioned in Section 9.2). If we arrive at the element u, then u is obviously primitive. What is not so obvious is what happens if we arrive at a *different* element; call it v.

We are going to show now that if $v \neq u$, then u is not primitive in A_2. By means of contradiction, suppose u is primitive. Let $\psi \in \mathrm{Aut}(A_2)$ take x_1 to u. Furthermore, let $\varphi(x_1) = v$ in A_2, so that $\varphi(x_1) = u^a$ in P_2 (we use the same letter for an automorphism $\varphi \in \mathrm{Aut}(A_2)$ and its natural image in $\mathrm{Aut}(P_2)$).

Since $u^a = v^a$, this yields $\varphi(x_1) = \psi(x_1)$ in P_2. By [80, Theorem 8.5], this implies $\varphi = \psi(\alpha)$ for some $\alpha \in \mathrm{Aut}(P_2)$ of the form $\{x_1 \to x_1;\ x_2 \to x_2 + f(x_1)\}$. This means $\varphi = \psi(\alpha)$ also in $\mathrm{Aut}(A_2)$.

But α, as well as its fellow automorphism of A_2, doesn't change x_1; hence $\psi(\alpha)(x_1) = \psi(x_1)$ both in P_2 and A_2. Therefore, we have in A_2 that $v = \varphi(x_1) = \psi(\alpha)(x_1) = \psi(x_1) = u$, a contradiction.

Therefore, u was not primitive in A_2, and this completes the proof of Theorem 9.2.2. ■

Proof of Proposition 9.2.3.

(i) It is clearly sufficient to prove this statement for linear automorphisms and for automorphisms of the form $\{x_1 \to x_1 + x_2^k;\ x_2 \to x_2\}$ and $\{x_1 \to x_1;\ x_2 \to x_2\}$, $k \geq 2$.

For linear automorphisms, the statement is obvious since J_2 is a K-linear subspace of A_2.

Since any power of x_1 and x_2 belongs to J_2, we have $\varphi(x_1), \varphi(x_2) \in J_2$ for any elementary automorphism φ. Now, by an obvious inductive argument, we have $(\varphi(uv + vu))^{\leftarrow} = \varphi(uv + vu)$, provided $(\varphi(u))^{\leftarrow} = \varphi(u)$ and $(\varphi(v))^{\leftarrow} = \varphi(v)$. Therefore, $\varphi(uv + vu)$ belongs to J_2 by [73]. The case when $\operatorname{char} K = 2$ is treated similarly.

(ii) As we have just seen, every automorphism of A_2 induces an automorphism of J_2; this mapping is obviously injective. Conversely, if φ is an automorphism of J_2, then $\varphi(x_1)$ and $\varphi(x_2)$ generate the algebra J_2 and hence also generate A_2. The result follows. ■

Proof of Proposition 9.2.6. We are going to show that there is the following "mirror symmetry" between left and right Fox derivatives for any $u \in A_2$ (it actually holds in a free associative algebra of arbitrary rank):

$$D_i(u^{\leftarrow}) = (d_i(u))^{\leftarrow}. \tag{9.10}$$

Without loss of generality, we can assume $u \in \Delta$, so let $u = \sum d_i(u) \cdot x_i$. Then $u^{\leftarrow} = \sum x_i \cdot (d_i(u))^{\leftarrow}$ and hence $(d_i(u))^{\leftarrow} = D_i(u^{\leftarrow})$, proving the equality (9.10).

Combining (9.10) with Lemma 9.2.7 and Corollary 9.2.5 yields the result. ■

9.3 Density of Coordinates in Polynomial Algebras

The exposition in this section follows [107].

Let K be a field of characteristic 0. In this section, we establish the following amazing fact: the set of coordinate polynomials of $K[X] = K[x_1, \ldots, x_n]$ is "dense" in the set of polynomials of the form $(x_i + q)$, $\deg(q) \geq 2$:

Theorem 9.3.1. *For any polynomial h of the form (x_i+q), $\deg(q) \geq 2$, and any integer $m \geq 2$, there is a coordinate polynomial p such that $\deg(p-h) > m$.*

This contrasts sharply with the situation in other, noncommutative algebraic systems; for example, the set of primitive elements (that is what generators are usually called in a noncommutative setting) of a free Lie algebra is not dense (see, e.g., [105]). Moreover, although the automorphism groups of $K[x_1, x_2]$ and $K\langle x_1, x_2\rangle$ (the free associative algebra of rank 2) are isomorphic, we have:

Proposition 9.3.2. *The element $u = x_1 + x_1x_2$ cannot be completed to a primitive element of $K\langle x_1, x_2\rangle$ by monomials of degree higher than 2.*

Our proof of Theorem 9.3.1 is based on some results of Anick [16] and that of Proposition 9.3.2 on a characterization of automorphisms of $K\langle x_1, x_2\rangle$ as it appears in [350].

First we have to give some more background on polynomial automorphisms. Anick [16] proved that, with respect to the formal power series topology (Zarisky topology), the set **J** of endomorphisms of $K[X]$ with an invertible Jacobian matrix is a closed set, and the group of tame automorphisms of $K[X]$ is dense in **J**. This means that for any polynomial mapping $F = (f_1, \ldots, f_n)$ with $0 \neq J(F) \in K$ and for any positive integer k there is a tame automorphism $G = (g_1, \ldots, g_n)$ such that the polynomials $(f_i - g_i)$ contain no monomials of degree less than k. Bryant, Drensky, and C. K. Gupta [61, 105] developed a technique based on representation theory of the general linear group $\mathrm{GL}_n(K)$ to study the automorphisms of some (commutative and noncommutative) algebras. An interpretation of the result of Anick in this language is given in [102, Theorem 4.2.7]. We recall some details here briefly.

Let P_k be a K-vector space of all homogeneous polynomials of degree $k \geq 0$. Let I_k, $k \geq 2$, be the semigroup of all polynomial endomorphisms $F = (f_1, \ldots, f_n)$ such that x_i is the only monomial of f_i of degree less than k; $i = 1, \ldots, n$. We write

$$f_i = x_i + g_i + h_i,$$

where $g_i \in P_k$ is the homogeneous component of f_i of degree k, and h_i has no monomials of degree $\leq k$. The group $\mathrm{GL}_n(K)$ acts on I_k by conjugation.

It turns out that there is a homomorphism φ of I_k onto the direct sum of additive groups $P_k^{\oplus n} \cong P_k \oplus \cdots \oplus P_k$ such that $\varphi(F) = (g_1, \ldots, g_n)$. It has been established that the action of $\mathrm{GL}_n(K)$ induced by φ on $\varphi(I_k)$ gives a structure of a $\mathrm{GL}_n(K)$-module to $\varphi(I_k)$.

Let T be the group of tame automorphisms of the algebra $K[X]$, and let $\mathbf{S}_k$ be the set of all polynomial mappings $S = (s_1, \ldots, s_n) \in I_k$ such that $s_i = x_i + g_i + h_i$, where $g_i \in P_k$ and $h_i \in \sum_{l>k} P_l$, with the property

$$\sum_{i=1}^{n} \frac{\partial g_i}{\partial x_i} = 0.$$

The main step of Anick's proof (see [102], Step 2 of the proof of Theorem 4.2.7) is to show that

$$\varphi(T \cap I_k) = \varphi(\mathbf{S}_k).$$

This yields the following lemma:

Lemma 9.3.3. *For any $S \in \mathbf{S}_k \subseteq I_k$, there is a tame automorphism G_k of $K[X]$ such that $S \circ G_k^{-1}$ is in I_{k+1}.*

Proof of Theorem 9.3.1. Let u be any polynomial without constant and linear terms, and let u_i be the homogeneous component of degree i of the polynomial u; $i = 2, \ldots, m$. Let k be the smallest integer such that $u_k \neq 0$.

Write the partial derivative of u_k with respect to x_1 in the form

$$\frac{\partial u_k}{\partial x_1} = \sum_{j=0}^{k-1} a_j x_2^j,$$

where polynomials a_j do not depend on x_2. There is a homogeneous polynomial $w_k \in P_k$ such that

$$\frac{\partial w_k}{\partial x_2} = -\sum_{j=0}^{k-1} a_j x_2^j.$$

Consider an endomorphism F_k of the algebra $K[X]$ defined by

$$F_k = (x_1 + u_k, x_2 + w_k, x_3, \ldots, x_n).$$

Clearly, $F_k \in I_k$ and, because of the choice of w_k, also $F_k \in \mathbf{S}_k$. Hence, by Lemma 9.3.3, there is a tame automorphism $G_k = (g_{1,k}, \ldots, g_{n,k}) \in I_k$ such that $F_{k+1} = F_k \circ G_k^{-1} \in I_{k+1}$. Therefore, $g_{1,k} = x_1 + u_k + v_{k+1} + v$, where v_{k+1} is homogeneous, of degree $k+1$, and $v \in \sum_{l \geq k+2} P_l$.

Continuing this way, we obtain a tame automorphism $G_{k+1} \in I_{k+1}E$ such that $g_{1,k+1} = x_1 + (u_{k+1} - v_{k+1}) + w$, where $w \in \sum_{l \geq k+2} P_l$.

If we act by the automorphism G_{k+1} on the polynomial u_k, we get a polynomial of the form $u_k + s$, where s has no homogeneous components of degree less than $(k-1)+(k+1) = 2k > k+1$. Therefore, the automorphism $G_{k+1} \circ G_k$ takes x_1 to $x_1 + u_k + u_{k+1} +$ (terms of higher degree).

In a finite number of steps, we obtain a tame automorphism $G = (g_1, \ldots, g_n)$ such that

$$g_1 = x_1 + u + \text{(terms of higher degree)}.$$

This completes the proof of Theorem 9.3.1. ■

Proof of Proposition 9.3.2. By way of contradiction, suppose there is an element $w \in \Delta^3$ such that $u = x_1 + x_1x_2 + w$ is a primitive element of $K\langle x_1, x_2 \rangle$.

By Lemma 9.2.7, we have

$$d_2(u) \cdot D_1(u) - d_1(u) \cdot D_2(u) = 0. \tag{9.11}$$

Now evaluate: $d_1(u) = 1 + d_1(w) = 1 + x_1 \pmod{\Delta^2}$; $d_2(u) = x_1 + d_2(w) = x_1 \pmod{\Delta^2}$; $D_1(u) = 1 + x_2 + D_1(w) = 1 + x_2 \pmod{\Delta^2}$; $D_2(u) = D_2(w) = 0 \pmod{\Delta^2}$.

Plugging this into (9.11) gives

$$x_1(1 + x_2) = 0 \pmod{\Delta^2},$$

a contradiction. ■

A combination of Theorem 9.3.1 and Proposition 9.3.2 calls for an example of a coordinate polynomial $p \in K[x_1, x_2]$ of the form $x_1 + x_1x_2 +$ (terms of higher degree); an example like that is given below.

Example 9.3.4. The following polynomial $p = x_1 + x_1x_2 + \frac{1}{4}(x_1x_2^2 - x_1^2x_2 - x_1^3 + x_2^3) - \frac{1}{16}(x_1 + x_2)^4$ is coordinate since it is the image of x_1 under an automorphism $\alpha\beta\alpha^{-2}\beta\alpha$, where α takes x_1 to $(x_1 + x_2)$ and fixes x_2, and β fixes x_1 and takes x_2 to $(x_2 - \frac{x_1^2}{4})$.

9.4 Coordinates in $K[z][x,y]$

The exposition in this section follows [112].

A well-known theorem of Jung and van der Kulk [164, 194] says that all automorphisms of the polynomial algebra $K[x,y]$ in two variables over a field K are tame; i.e., they can be decomposed as products of affine and triangular automorphisms. A combinatorial description of $\mathrm{Aut}(K[x,y])$ as the amalgamated free product of the subgroups of affine and upper triangular automorphisms is also well-known (see the book by Cohn [80]). Several algorithms have been discovered that determine whether a homomorphism of $K[x,y]$ is an automorphism and, if it is, decompose it as a product of linear and triangular automorphisms (see [69, 80, 119]). Results of [359] over a field of characteristic 0 give that one can also determine whether a polynomial $p(x,y) \in K[x,y]$ is a coordinate (i.e., if it is the image of x under some automorphism $P = (p,q)$ of $K[x,y]$) and to find a concrete P with this property.

On the other hand, very little is known about automorphisms of the polynomial algebra $R[x,y]$, where R is a commutative algebra. The first result in this direction was the famous example of Nagata [288] of an automorphism of the $K[z]$-algebra $K[z][x,y]$, which is not tame. Then Wright [404] described the structure of the group of tame automorphisms of $R[x,y]$ over any principal ideal domain as an amalgamated free product in the same way as over a field. Wright showed also that the group of all automorphisms of $R[x,y]$ is an amalgamated free product of the affine group and one more group of automorphisms that, when R is not a field, properly contains the group of upper triangular automorphisms.

Recently, Lam and Yu [200] have obtained algorithms: (i) for recognizing coordinates of $D[x,y]$, where D is a unique factorization domain; (ii) for recognizing tame coordinates of $R[x,y]$, where R is an Euclidean domain. These algorithms are applicable, in particular, to polynomials from $\mathbb{Z}[x,y]$.

The purpose of this section is to study $K[z]$-automorphisms and coordinates of $K[z][x,y]$, where K is a field of characteristic 0. Applying results of [404] for $K[z][x,y]$ and of [359] for $K[x,y]$, we characterize tame coordinates of $K[z][x,y]$. Specifically, a polynomial $p(x,y) \in K[z][x,y]$ is a tame coordinate if and only if 1 can be obtained from the partial derivatives $p_x = \partial p/\partial x$ and $p_y = \partial p/\partial y$ using the Euclidean algorithm. Hence the problem of whether a polynomial $p(x,y) \in K[z][x,y]$ is a tame coordinate can be solved by using division of polynomials only. In particular, our al-

gorithm produces a concrete tame automorphism of $K[z][x,y]$ sending x to $p(x,y)$. We also use recent results of Daigle and Freudenburg [87] on locally nilpotent derivations and characterize coordinates of $K[z][x,y]$ (i.e., images of x under automorphisms of $K[z][x,y]$). Namely, we show that $p(x,y) \in K[z][x,y]$ is a coordinate in $K[z][x,y]$ if and only if $p(x,y)$ is a coordinate as an element of $K(z)[x,y]$ and has a unimodular gradient, which means that $K[z][x,y]$ is generated as an ideal by the partial derivatives p_x and p_y. As in the tame case, our approach allows us to solve effectively the problem of whether a polynomial is a coordinate, but this time we have to apply Gröbner basis techniques instead of the Euclidean algorithm.

The Nagata automorphism was recently proved to be wild when considered as an automorphism of the polynomial algebra $K[x,y,z]$ in three variables; see [343]. On the other hand, M. Smith [370] discovered another important property of the Nagata automorphism. She showed that it is stably tame and becomes tame if we extend it to an automorphism of $K[z][x,y,t]$ fixing t.

Considered as an automorphism of $K(z)[x,y]$, the Nagata automorphism is a conjugate of an elementary automorphism by another elementary automorphism. Hence, the Nagata automorphism is a product of three elementary automorphisms of $K(z)[x,y]$. We study automorphisms of $K[z][x,y]$ that have a similar presentation. In particular, we consider polynomials of the form $p(x,y) = x + q(a(x) + by)$, where $q(w) \in K[z][w]$, $a(x) \in K[z][x]$, $b \in K[z]$, and study the problem when these polynomials are coordinate in $K[z][x,y]$. We establish that if $q(w)$ is divisible by all irreducible factors of $b(z)$, then p is coordinate and is the image of x under an automorphism that is a product of three elementary automorphisms of $K(z)[x,y]$. In the special case where $q(w)$ is divisible by $b(z)$ itself, we show that p is really a "Nagata-like" coordinate and is the image of an automorphism of $K[z][x,y]$ that is a conjugate of an elementary automorphism by another elementary automorphism of $K(z)[x,y]$. We also show that automorphisms with $q(w)$ divisible by $b(z)$ are stably tame. In this way, our results give a new large family of automorphisms of $K[z][x,y]$ that may be considered as candidates of wild automorphisms of $K[x,y,z]$. In fact, Umirbaev and Yu [393] have recently proved the following

Theorem 9.4.1 ([393]). *Any wild coordinate of $K[z][x,y]$ is also a wild coordinate of $K[x,y,z]$.*

This result therefore enhances the importance of producing wild coordinates in $K[z][x,y]$.

9.4.1 Preliminaries

We fix a field K of characteristic 0 and, if not explicitly stated, consider commutative unitary K-algebras only. If R is an algebra, we denote by $R[x,y]$ the polynomial algebra in two variables x, y over R. Sometimes we

use the notation p_x and p_y, respectively, for the partial derivatives $\partial p/\partial x$ and $\partial p/\partial y$ of $p \in R[x,y]$. In what follows, we assume that R is one of the algebras K, $K[z]$, or $K(z)$. We denote the endomorphisms of $R[x,y]$ as $F = (f_1(x,y), f_2(x,y))$ assuming that f_1 and f_2 are respectively the images of x and y (and that F is an R-algebra endomorphism). If F is an automorphism, then its inverse is denoted by F^{-1}. We use similar notation for endomorphisms of polynomial algebras in more than two variables. The Jacobian matrix of $F = (f_1, f_2) \in \operatorname{End} R[x,y]$ is

$$J_F = J_F(x,y) = \begin{pmatrix} \partial f_1/\partial x & \partial f_1/\partial y \\ \partial f_2/\partial x & \partial f_2/\partial y \end{pmatrix}.$$

The composition $F \circ G$ of two endomorphisms $F = (f_1, f_2)$ and $G = (g_1, g_2)$ is

$$F \circ G = F(G) = (f_1(g_1, g_2), f_2(g_1, g_2)).$$

The chain rule gives that

$$J_{F \circ G}(x,y) = J_F(g_1, g_2) J_G(x,y).$$

In particular, if F is an automorphism, then its Jacobian matrix is invertible over R.

Now we refresh some definitions.

Definition 9.4.2. An automorphism of $R[x,y]$ is called *tame* if it belongs to the subgroup of $\operatorname{Aut}(R[x,y])$ generated by affine automorphisms and triangular automorphisms, the latter being defined as

$$F = (\alpha x + f(y), \beta y),$$

where $\alpha, \beta \in R^*$ and $f \in R[y]$ is a polynomial that does not depend on x. Automorphisms that are not tame are called *wild*.

Remark 9.4.3. The notion of tame and wild automorphisms depends on the ground algebra R. For example, Nagata [288] constructed the automorphism of $K[x,y,z]$ defined by

$$N = (x - 2(y^2 + zx)y - (y^2 + zx)^2 z, y + (y^2 + zx)z, z),$$

which is wild when considered as an automorphism of $K[z][x,y]$. Only recently was it proved [343] that N is wild as an automorphism of $K[x,y,z]$.

Definition 9.4.4. Any automorphic image $p = p(x,y) \in R[x,y]$ of x is called a *coordinate polynomial* or simply a *coordinate*. If $P = (p,q)$ for some tame automorphism P of $R[x,y]$, then p is a *tame coordinate*. If all automorphisms P that send x to p are wild, then the coordinate p is also called *wild*.

Remark 9.4.5. If p is a tame coordinate of $R[x,y]$, then all automorphisms Q of $R[x,y]$ with the property $Q = (p,q)$ are tame. Indeed, if $P = (p, q_0)$ for some tame automorphism P of $R[x,y]$ and $Q = (p,q) \in$

$\mathrm{Aut}(R[x,y])$, then the automorphism $S = Q \circ P^{-1}$ fixes x. It is easy to see that $S = (x, \alpha y + g(x))$ for some $\alpha \in R^*$ and $g(x) \in R[x]$; i.e., S is tame. Since P is also tame, this implies that Q is tame.

Let $\mathrm{GE}_2(R[x,y])$ be the subgroup of $\mathrm{GL}_2(R[x,y])$ generated by elementary and diagonal matrices. By the Jung–van der Kulk theorem and the chain rule, the Jacobian matrix of every automorphism of $K[x,y]$ belongs to $\mathrm{GE}_2(K[x,y])$. On the other hand, the weak Jacobian theorem of Wright states that if the Jacobian matrix of an endomorphism F of $K[x,y]$ belongs to $\mathrm{GE}_2(K[x,y])$, then F is an automorphism. This result was generalized to coordinate polynomials by Shpilrain and Yu [359]. They showed that $p(x,y) \in K[x,y]$ is a coordinate polynomial if and only if the vector $(\partial p/\partial x, \partial p/\partial y)$ is the first row of some matrix in $\mathrm{GE}_2(K[x,y])$. An equivalent form of this statement is that $(\partial p/\partial x, \partial p/\partial y)$ can be brought to $(1,0)$ by a Euclidean algorithm.

The results of Wright [404] and Shpilrain and Yu [359] are based on the description of the group $\mathrm{GE}_2(K[x_1,\dots,x_n])$ as an amalgamated free product. Recall the definition of an amalgamated free product (see, e.g., [231] or [404]). If A, B, and C are three abstract groups such that $\varphi\colon B \to A$ and $\psi\colon B \to C$ are two embeddings, then the amalgamated free product $G = A *_B C$ is generated by $A \cup C$, and the defining relations of G are the defining relations of A and C together with the defining relations $\varphi(b) = \psi(b)$, $b \in B$. If we consider B as a subgroup of A and C and assume that $A \cap C = B$, then the elements of $G = A *_B C$ can be presented as

$$g = b a_1^{\varepsilon_1} c_1 a_2 c_2 \dots a_k c_k^{\varepsilon_2},$$

where $b \in B$, $a_i \in A$, $c_i \in C$, and ε_1, ε_2 are equal to 1 or 0, depending on whether or not a_1 and c_k occur in the expression of g. It is well-known that g is different from 1, provided that $a_1,\dots,a_k$ and $c_1,\dots,c_k$ do not belong to B. The description of $\mathrm{GE}_2(K[x_1,\dots,x_n])$ given by Wright [404] is the following.

Theorem 9.4.6 ([404]). *The group* $\mathrm{GE}_2(K[x_1,\dots,x_n])$ *is isomorphic to the amalgamated free product of the subgroup* $\mathrm{GL}_2(K)$ *and the subgroup* $B_2(K[x_1,\dots,x_n])$ *of all lower triangular matrices with polynomial entries.*

We assume that we can perform concrete calculations with the elements of K. We also introduce an arbitrary ordering on the monomials of $K[x,y,z]$ that allows us to make induction and is preserved under multiplication. For example, we may consider the usual lexicographic ordering or the *deg-lex ordering*, comparing the monomials of $K[x,y,z]$ first by total degree and then lexicographically with $x > y > z$. (See, e.g., [13] for different orderings of $K[x_1,\dots,x_n]$.) We say that a matrix

$$a = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GE}_2(K[x,y,z])$$

can be decomposed into a product of diagonal and elementary matrices using a Euclidean algorithm if, in each step of bringing a to its diagonal form by elementary transformations, we multiply it on the right by an elementary matrix that decreases the leading terms of the first row of a. For example, if the leading term of a_{11} is equal to the leading term of ba_{12} for some monomial $b \in K[x,y,z]$, then we are allowed to replace a by

$$ua = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}.$$

In particular, if f and g are two relatively prime polynomials in $K[x,y,z]$ and we reach 1 by applying the usual Euclidean algorithm to f and g, then the corresponding operations can be written in a matrix form as

$$\begin{pmatrix} a_{11} & a_{12} \end{pmatrix} e_1 \dots e_k = \alpha \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \alpha \in K^*,$$

where $e_1, \dots, e_k$ are (alternatively lower and upper) triangular matrices

$$e_i = \begin{pmatrix} 1 & h_i \\ 0 & 1 \end{pmatrix}, \quad e_{i+1} = \begin{pmatrix} 1 & 0 \\ h_{i+1} & 1 \end{pmatrix}.$$

We shall make use of a result of the thesis of Park [297]. Since the journal version of [297] has not been published yet, a proof for the case of polynomials in two variables can be found in [359]. A careful study of the proof in [359] shows that it works for any number of variables and any ordering.

Proposition 9.4.7. *Every matrix in* $\mathrm{GE}_2(K[x,y,z])$ *can be decomposed into a product of diagonal and elementary matrices by using a Euclidean algorithm only.*

Remark 9.4.8. If (f,g) is a pair of polynomials brought to $(1,0)$ by the Euclidean algorithm in k steps

$$\begin{pmatrix} a_{11} & a_{12} \end{pmatrix} e_1 \dots e_k = \alpha \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \alpha \in K^*,$$

then the matrix $e_1 \dots e_k$ belongs to $\mathrm{GE}_2(K[x,y,z])$, and one presentation as an element of $\mathrm{GL}_2(K) *_{B_2(K)} B_2(K[x,y,z])$ can be obtained by replacing the upper triangular matrices $(e_{11} + e_{22}) + h_i e_{12}$ by the products $((e_{11} + e_{22}) + h_i e_{21})(e_{12} + e_{21})$ if h_i is not a constant.

9.4.2 Characterization of tame and wild coordinates in $K[z][x,y]$

In this section, we characterize tame coordinates in $K[z][x,y]$. Then we give algorithms that recognize whether a polynomial $p(x,y) \in K[z][x,y]$ is a tame coordinate and, if it is, find concrete tame automorphisms sending x to $p(x,y)$. Finally, we characterize all coordinates in $K[z][x,y]$ and give a procedure that determines whether a polynomial is a coordinate of $K[z][x,y]$. In particular, we are able to find effectively a lot of wild

automorphisms of $K[z][x,y]$, giving in this way new candidates for wild automorphisms of $K[x,y,z]$, all of them fixing z as in the example suggested by Nagata.

To prove our main results on tame automorphisms, we modify the considerations in the proof of the weak Jacobian theorem in [404] and the description of the coordinate polynomials in $K[x,y]$ in [359].

Lemma 9.4.9. *Let $\xi\colon K[x,y,z] \to \mathbb{Z}^3$ be the degree function on $K[x,y,z]$ induced by the lexicographic ordering $x > y > z$; i.e., $\xi(f) = (d_1,d_2,d_3)$ if the leading term of $f \neq 0$ is $\alpha x^{d_1}y^{d_2}z^{d_3}$, $\alpha \in K^*$. Let $a_1,\dots,a_k$ be matrices in $\mathrm{GL}_2(K)$ that do not belong to the lower triangular group $B_2(K)$, and let $c_i = (e_{11}+e_{22}) + f_i e_{21}$, $i = 1,\dots,k$, where $f_1,\dots,f_k$ are polynomials of positive degree. Then the row-matrices*

$$\begin{pmatrix} u_0 & v_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} u_i & v_i \end{pmatrix} = \begin{pmatrix} u_{i-1} & v_{i-1} \end{pmatrix} a_i c_i,$$

$i = 1,\dots,k$, satisfy the equation

$$\xi(u_i) = \xi(v_i) + \xi(f_i).$$

Proof. We use induction on i. If $a_1 = \alpha_{11}e_{11} + \alpha_{12}e_{12} + \alpha_{21}e_{21} + \alpha_{22}e_{22}$, $\alpha_{12} \neq 0$, then direct calculations show that

$$u_1 = \alpha_{11} + \alpha_{12}f_1, \quad v_1 = \alpha_{12},$$

and $\xi(u_1) = \xi(f_1)$, $\xi(v_1) = \xi(\alpha_{12}) = (0,0,0)$. Similarly, if $a_i = \beta_{11}e_{11} + \beta_{12}e_{12} + \beta_{21}e_{21} + \beta_{22}e_{22}$, $\beta_{12} \neq 0$, then

$$u_i = (\beta_{12}f_i + \beta_{11})u_{i-1} + (\beta_{22}f_i + \beta_{21})v_{i-1}, \quad v_i = \beta_{12}u_{i-1} + \beta_{22}v_{i-1},$$

and $\xi(u_i) = \xi(u_{i-1}) + \xi(f_i)$, $\xi(v_i) = \xi(u_{i-1})$, which completes the proof by induction. ∎

The following theorem is one of the main results of this section.

Theorem 9.4.10. *The following statements for $p(x,y) \in K[z][x,y]$ are equivalent:*

(i) *The polynomial $p(x,y)$ is a tame coordinate of $K[z][x,y]$.*

(ii) *There exists a matrix $g \in \mathrm{GE}_2(K[x,y,z])$ such that*

$$\begin{pmatrix} p_x & p_y \end{pmatrix} g = \begin{pmatrix} 1 & 0 \end{pmatrix};$$

i.e., $\begin{pmatrix} p_x & p_y \end{pmatrix}$ can be brought to $\begin{pmatrix} 1 & 0 \end{pmatrix}$ by elementary transformations.

(iii) *When applying a Euclidean algorithm to p_x and p_y, the result is equal to 1.*

Proof. The equivalence of (ii) and (iii) follows immediately from Proposition 9.4.7. The implication (i) $\Longrightarrow$ (ii) is a consequence of the chain rule and the fact that $K[z]$ is a Euclidean domain (hence $\mathrm{GE}_2(K[z]) = \mathrm{GL}_2(K[z])$ and the Jacobian matrix of any affine automorphism of $K[z][x,y]$ belongs

to $\mathrm{GE}_2(K[x,y,z])$). Therefore, it is sufficient to show that (ii) implies (i). Let

$$\begin{pmatrix} p_x & p_y \end{pmatrix} g = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

for some matrix $g = g(x,y) \in \mathrm{GE}_2(K[x,y,z])$ (depending on x, y and on the "constant" z) and let

$$g = a_1 c_1 a_2 c_2 \dots a_k c_k^{\varepsilon},$$

where $a_1, \dots, a_k \in \mathrm{GL}_2(K)$ and $a_2, \dots, a_k$ do not belong to the lower triangular group $B_2(K)$, $c_i = (e_{11} + e_{22}) + f_i e_{21}$ for some nonconstant polynomials $f_i \in K[x,y,z]$, $i = 1, \dots, k$, and $\varepsilon = 0, 1$. Since

$$\begin{pmatrix} u & v \end{pmatrix} \begin{pmatrix} 1 & 0 \\ f_k & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

implies that $\left(\begin{smallmatrix} u & v \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \end{smallmatrix}\right)$, without loss of generality we may assume that $\varepsilon = 0$. Let

$$a_1 = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}, \quad g(x,y) = a_1 g_1(x,y),$$
$$q(x,y) = p(\alpha_{11}x + \alpha_{12}y, \alpha_{21}x + \alpha_{22}y).$$

Replacing x and y, respectively, by $\alpha_{11}x + \alpha_{12}y$ and $\alpha_{21}x + \alpha_{22}y$ in $\left(\begin{smallmatrix} p_x & p_y \end{smallmatrix}\right) g(x,y) = \left(\begin{smallmatrix} 1 & 0 \end{smallmatrix}\right)$, easy computation shows that $\left(\begin{smallmatrix} p_x & p_y \end{smallmatrix}\right) a_1$ goes to $\left(\begin{smallmatrix} q_x & q_y \end{smallmatrix}\right)$ (i.e., to the gradient of $q(x,y)$), and we obtain a new equation

$$\begin{pmatrix} q_x & q_y \end{pmatrix} g'(x,y) = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad g'(x,y) = g_1(\alpha_{11}x + \alpha_{12}y, \alpha_{21}x + \alpha_{22}y),$$

where the decomposition $g' = c_1 a_2 \dots c_{k-1} a_k$ starts with c_1. Let ξ be the degree function on $K[x,y,z]$ induced by the lexicographic ordering $x > y > z$. Since

$$\begin{pmatrix} q_x & q_y \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix} a_k^{-1} c_{k-1}^{-1} \dots a_2^{-1} c_1^{-1}$$

and $c_1^{-1} = (e_{11} + e_{22}) - f_1 e_{21}$, Lemma 9.4.9 gives that $\xi(q_x) = \xi(q_y) + \xi(f_1)$. First, we assume that f_1 essentially depends on x. Let, for example, $\xi(q_y) = (d_1, d_2, d_3)$, $\xi(f_1) = (e_1, e_2, e_3)$, and $e_1 > 0$. Then $\xi(q_x) = (d_1 + e_1, d_2 + e_2, d_3 + e_3)$. Since $q_{xy} = q_{yx}$, we obtain that $\xi(q_{xy}) = (d_1 + e_1 - 1, d_2 + e_2, d_3 + e_3)$ and $\xi(q_{yx}) = (d_1, d_2 - 1, d_3)$ if $d_2 > 0$, or $\xi(q_{yx}) \le (d_1 - 1, d_2', d_3')$ for some d_2', d_3' if $d_2 = 0$. Since this is impossible, we derive that f_1 does not depend on x. Let $f(y) \in K[z][y]$ be a polynomial such that $f_y = f_1$. Replacing x by $x + f(y)$ in the equation $\left(\begin{smallmatrix} q_x & q_y \end{smallmatrix}\right) g_1 = \left(\begin{smallmatrix} 1 & 0 \end{smallmatrix}\right)$, we obtain that $\left(\begin{smallmatrix} q_x & q_y \end{smallmatrix}\right) c_1$ goes to the gradient of $p_1(x,y) = q(x + f(y), y)$. In this way we obtain the equation $\left(\begin{smallmatrix} (p_1)_x & (p_1)_y \end{smallmatrix}\right) g_2 = \left(\begin{smallmatrix} 1 & 0 \end{smallmatrix}\right)$, where $g_2 = a_2 c_2 \dots c_{k-1} a_k$. By inductive arguments, we may assume that $p_1(x,y)$ is a tame coordinate. Since both $A_1 = (\alpha_{11}x + \alpha_{12}y, \alpha_{21}x + \alpha_{22}y)$ and $F_1 = (x + f(y), y)$ are tame automorphisms, we obtain that $p(x,y)$ is also a tame coordinate.

■

Remark 9.4.11. The theorem of Wright about the structure of the group $\mathrm{GE}_2(K[z][x,y])$ holds for any Euclidean domain R in place of $K[z]$. Nevertheless, the proof of Theorem 9.4.10 does not hold for Euclidean domains R of characteristic 0 that do not contain the field $\mathbb{Q}$. The reason is that in the inductive step of the proof we have used that the integral of the polynomial $f(y) \in K[z][y]$ also belongs to $K[z][y]$. For instance, Theorem 9.4.10 is no longer true even for $R = \mathbb{Z}$. A simple example is the following. If we replace in the Nagata automorphism

$$N = (x - 2(y^2 + zx)y - (y^2 + zx)^2 z, y + (y^2 + zx)z) \in \mathrm{Aut}\, K[z][x,y]$$

z by 2, we obtain the automorphism

$$N_0 = (p,q) = (x - 2(y^2 + 2x)y - 2(y^2 + 2x)^2, y + 2(y^2 + 2x)) \in \mathrm{Aut}\, \mathbb{Z}[x,y],$$

and $p_x = 1 - 4(y + 2(y^2 + 2x))$, $p_y = -4y(y + 2(y^2 + 2x)) - 2(y^2 + 2x)$,

$$p_y - yp_x = -y - 2(y^2 + 2x), \quad p_x - 4(p_y - yp_x) = 1.$$

Similarly, $q_x = 4$, $q_y = 1 + 4y$, $q_y - yq_x = 1$. Hence both p and q satisfy the hypothesis of Theorem 9.4.10 (iii). On the other hand, we shall see that N_0 is a wild automorphism of $\mathbb{Z}[x,y]$. Following the proof of Wright [404, p. 247] for existence of wild automorphisms of $R[x,y]$ where R is a principal ideal domain that is not a field, our considerations are the following. Let

$$I = \{A_i = (\alpha_i x + \beta_i y, \alpha_i' x + \beta_i' y)\}$$

be a set of nontrivial left coset representatives of

$$\mathrm{GL}_2(\mathbb{Q}) = \{F = (\alpha x + \beta y, \alpha' x + \beta' y) \mid \alpha, \beta, \alpha', \beta' \in K,\ J_F \text{ invertible}\}$$

considered as a subgroup of $\mathrm{Aut}(\mathbb{Q}[x,y])$ modulo $B_2(\mathbb{Q}) = \{(\alpha x + \beta y, \alpha' x) \mid \alpha, \alpha' \in \mathbb{Q}^*,\ \beta \in \mathbb{Q}\}$. (Comparing with [404], we change left and right for cosets and lower and upper for triangular automorphisms because of the difference in the definitions of $F \circ G$ and J_F.) As in [404], we can choose I as a subset of $\mathrm{GL}_2(\mathbb{Z})$. Let also

$$J = \{C = (x + y^2 f(y), y) \mid f \in \mathbb{Q}\}$$

be the set of triangular automorphisms of $\mathbb{Q}[x,y]$ corresponding to polynomials without linear components. Then the set W of all automorphisms

$$P = C_1 \circ A_1 \circ C_2 \circ \cdots \circ A_{k-1} \circ C_k \circ B,$$

such that $A_i \in I$, $C_i \in J$, $B \in B_2(\mathbb{Z})$, and $C_1 \circ A_1 \circ \cdots \circ A_{l-1} \circ C_l$ is not an automorphism of $\mathbb{Z}[x,y]$ for $l < k$, is a subgroup of $\mathrm{Aut}(\mathbb{Z}[x,y])$. The subgroup $\mathrm{Aut}^0(\mathbb{Z}[x,y])$ of all automorphisms preserving the augmentation of $\mathbb{Z}[x,y]$ has the presentation

$$\mathrm{Aut}^0(\mathbb{Z}[x,y]) \cong \mathrm{GL}_2(\mathbb{Z}) *_{B_2(\mathbb{Z})} W.$$

In particular, if $P = C_1 \circ A_1 \circ \cdots \circ A_{k-1} \circ C_k \in W$ and $k > 1$, then P is a wild automorphism of $\mathbb{Z}[x,y]$. In our case, we choose I in such a way

that it contains $A = (x, y + 4x)$, we define $C = (x + y^2/2, y)$, and a direct calculation shows that $N_0 = C^{-1} \circ A \circ C$. Hence N_0 is a wild automorphism of $\mathbb{Z}[x,y]$.

Corollary 9.4.12. *There is an algorithm that determines whether a polynomial $p(x,y) \in K[z][x,y]$ is a tame coordinate and, if the answer is affirmative, produces a concrete tame automorphism of $K[z][x,y]$ that sends x to $p(x,y)$.*

Proof. Given a polynomial $p \in K[z][x,y]$, we want to decide whether it is a tame coordinate. The algorithm can be derived from the proof of Theorem 9.4.10. We fix some ordering in $K[x,y,z]$ (e.g., the lexicographic or the deg-lex ordering satisfying $x > y > z$).

Step 1. Take the partial derivatives $q_1 = p_x$, $q_2 = p_y$.

Step 2. If the leading monomial (l. m.) of q_1 is not divisible by the leading monomial of q_2 (or vice versa), then p is not a tame coordinate. If $\text{l. m.}(q_1) = h \cdot \text{l. m.}(q_2)$ (or $\text{l. m.}(q_2) = h \cdot \text{l. m.}(q_1)$) for some monomial $h \in K[z][x,y]$, then go to:

Step 3. Set $q_1' = q_1 - hq_2$ and $q_2' = q_2$ (or $q_1' = q_1$ and $q_2' = q_2 - hq_1$). If, say, $\text{l. m.}(q_1') = \alpha \in K^*$, then p is a tame coordinate of $K[z][x,y]$. If $\text{l. m.}(q_1') = 0$, then p is a tame coordinate if and only if $\text{l. m.}(q_2) = \alpha \in K^*$. If $\text{l. m.}(q_1') \notin K$, then repeat Step 2 upon replacing q_1 with q_1' and q_2 with q_2'.

The algorithm for constructing a tame automorphism of $K[z][x,y]$ that sends x to p is also contained in the proof of Theorem 9.4.10. For simplicity, we assume that we always know that $p = p(x,y)$ is a tame coordinate.

Step 1. Define an automorphism $T = (t_1(x,y), t_2(x,y)) = (x,y)$ of $K[z][x,y]$.

Step 2. Take $Q = (q_1, q_2) = (p_x, p_y)$.

Step 3. If one of the polynomials q_1 or q_2 is equal to a nonzero constant α, then $p = \alpha x + f(y)$ (or $p = \alpha y + f(x)$). Replace T by $T = (t_1(\alpha x + f(y), y), t_2(\alpha x + f(y)))$ (or by $T = (t_1(x, \alpha y + f(x)), t_2(x, \alpha y + f(x)))$). The automorphism T is the inverse of an automorphism of $K[z][x,y]$ that sends x to the initially given $p(x,y)$.

If neither q_1 nor q_2 is a constant, then let the result of the division of q_1 by q_2 be $q_1 = hq_2 + r$ (or $q_2 = hq_1 + r$). Then $h = h(y) \in K[z][y]$ does not depend on x (or $h = h(x) \in K[z][x]$ does not depend on y). Choose $f(y) \in K[z][y]$ such that $f_y = h(y)$ (or $f(x) \in K[z][x]$ such that $f_x = h(x)$). Replace $p(x,y)$ and T, respectively, by $p(x + f(y), y)$ and $T = (t_1(\alpha x + f(y), y), t_2(\alpha x + f(y), y))$ (or respectively by $p(x, y + f(x))$ and $T = (t_1(x, \alpha y + f(x)), t_2(x, \alpha y + f(x)))$). Then go to Step 2.

If we want to determine all automorphisms sending x to $p(x,y)$, we can use Remark 9.4.5. ∎

Now we apply our results to get similar algorithms in the free associative algebra over $K[z]$:

Corollary 9.4.13. *There is an algorithm that determines whether a polynomial $p(x,y)$ in the free associative algebra $K[z]\langle x,y\rangle$ is a tame coordinate and, if the answer is affirmative, produces a concrete tame automorphism sending x to $p(x,y)$.*

Proof. By the proof of Theorem 1.2 in [360], for every field R and every coordinate $q_0(x,y) \in R[x,y]$ there exists a unique coordinate $q_1(x,y) \in R\langle x,y\rangle$ that maps onto $q_0(x,y)$ under the natural homomorphism $R\langle x,y\rangle \to R[x,y]$. Since every tame automorphism of $K[z][x,y]$ is induced by a tame automorphism of $K[z]\langle x,y\rangle$, this implies that if $p_0(x,y) \in K[z][x,y]$ is a tame coordinate, then it is an image of a unique tame coordinate $p_1(x,y) \in K[z]\langle x,y\rangle$. Our algorithm for recognizing the tame coordinates in $K[z]\langle x,y\rangle$ is the following. If $p(x,y) \in K[z]\langle x,y\rangle$, take its image p_0 under the natural homomorphism $K[z]\langle x,y\rangle \to K[z][x,y]$. Apply the algorithm in Corollary 9.4.12 to p_0. If p_0 is not a tame coordinate in $K[z][x,y]$, then p is not a tame coordinate in $K[z]\langle x,y\rangle$. If p_0 is a tame coordinate in $K[z][x,y]$, then find a product of elementary automorphisms $F = (p_0, q_0) = F_1 \circ F_2 \circ \cdots \circ F_n$ that sends x to p_0. Take the preimage $G = (p_1, q_1)$ of F under the natural isomorphism $\mathrm{Aut}(K[z]\langle x,y\rangle) \to \mathrm{Aut}(K[z][x,y])$. Then p is a tame coordinate if and only if $p_1 = p$. ■

It is also interesting to characterize effectively all coordinates (in particular, nontame ones) in $K[z][x,y]$. The following theorem is based on recent results of Daigle and Freudenburg [87]. Recall that a derivation δ of $K[X] = K[x_1,\ldots,x_n]$ is called *locally nilpotent* if for any $u \in K[X]$ there exists a positive n such that $\delta^n(u) = 0$. Following [87, Definition 2.2], for any polynomial $p = p(x,y) \in K[z][x,y]$, we define a mapping $\Delta_p \colon K[z][x,y] \to K[z][x,y]$ by

$$\Delta_p = -p_y \frac{\partial}{\partial x} + p_x \frac{\partial}{\partial y};$$

i.e., $\Delta_p(f)$ is equal to the determinant of the Jacobian matrix of the endomorphism $F = (p, f)$ of $K[z][x,y]$, $f \in K[z][x,y]$. It is easy to see that Δ_p is locally nilpotent if p is a coordinate of $K(z)[x,y]$.

Theorem 9.4.14. *The polynomial $p = p(x,y) \in K[z][x,y]$ is a coordinate if and only if p is a coordinate in $K(z)[x,y]$ with unimodular gradient in $K[z][x,y]$.*

Proof. Clearly, if $p = p(x,y) \in K[z][x,y]$ is a coordinate of $K[z][x,y]$, then it is also a coordinate of $K(z)[x,y]$, and for every automorphism $F = (p,q)$ of $K[z][x,y]$ sending x to p, the determinant of the Jacobian matrix of F is a nonzero constant in K. Hence p has a unimodular gradient, and this gives the "easy" part of the theorem.

Now let $p \in K[z][x,y]$ be a coordinate in $K(z)[x,y]$ with a unimodular gradient in $K[z][x,y]$. Restricted to the case of $K[z][x,y]$, Proposition 2.3

of [87] states that every $p \in K[z][x,y]$ that is a coordinate in $K(z)[x,y]$ with a unimodular gradient in $K[z][x,y]$ has the property that the derivation Δ_p defined above is locally nilpotent and its kernel $\operatorname{Ker}\Delta_p$ is equal to $K[z][p]$. Since

$$\Delta_p(x) = -p_y, \quad \Delta_p(y) = p_x,$$

we obtain that the ideals of $K[z][x,y]$ generated, respectively, by the image of Δ_p and by p_x, p_y coincide and, by the unimodularity of the gradient, are equal to $K[z][x,y]$. By the implication (3) $\Longrightarrow$ (2) of [87, Theorem 2.5], every locally nilpotent derivation Δ of $K[z][x,y]$ such that the ideal of $K[z][x,y]$ generated by the image of Δ coincides with $K[z][x,y]$ satisfies also the condition $K[z][x,y] = (\operatorname{Ker}\Delta)[q]$ for some $q \in K[z][x,y]$. Hence

$$K[z][x,y] = (\operatorname{Ker}\Delta)[q] = (K[z][p])[q] = K[z][p,q].$$

Hence the endomorphism $F = (p,q)$ of $K[z][x,y]$ is an automorphism and p is a coordinate in $K[z][x,y]$. ■

Example 9.4.15. Let every irreducible factor of $b(z) \in K[z]$ be a divisor of $c(z) \in K[z]$, and let $a(x,z) \in K[x,z]$ be such that $b(z)$ does not divide some coefficient $a_i(z)$, $i > 0$, of $a_x = \sum_{i=0}^{n} a_i(z)x^i$. Then for any $q(u,z) \in K[u,z]$ with $\deg_u q > 0$, the polynomial $p(x,y,z) = x + q(a(x,z) + b(z)y, z)c(z)$ is a wild coordinate in $K[z][x,y]$.

Proof. Applying Theorem 9.4.10, we calculate

$$p_x = 1 + c(z)a_x q_u(a(x,z) + b(z)y, z),$$
$$p_y = b(z)c(z)q_u(a(x,z) + b(z)y, z).$$

It is easy to see that the first steps of a Euclidean algorithm for p_x and p_y in $K[x,y,z]$ are the same as for a_x and $b(z)$ in $K[x,z]$ and in this way we cannot reach 1 because some summand $a_i(z)x^i$ of a_x is not divisible by $b(z)$. Now, we apply Theorem 9.4.14. Since every irreducible factor of $b(z)$ divides $c(z)$, we obtain that no solution of the equation $p_y = 0$ in the algebraic closure of K is a solution of the equation $p_x = 0$. By Hilbert's Nullstellensatz, this implies that the ideal of $K[x,y,z] = K[z][x,y]$ generated by p_x and p_y is equal to $K[z][x,y]$. On the other hand, $p_x - a_x p_y/b = 1$ in $K(z)[x,y]$ and hence (see [359] or our Theorem 9.4.10) we obtain that p is a coordinate in $K(z)[x,y]$. ■

Corollary 9.4.16. *There is an algorithm that determines whether a polynomial $p(x,y) \in K[z][x,y]$ is a coordinate.*

Proof. Given a polynomial $p(x,y) \in K[z][x,y]$, we apply the following procedure.

Step 1. We choose some ordering on $K[x,y,z]$ and calculate the reduced Gröbner basis of the ideal of $K[x,y,z]$ generated by p_x and p_y (see e.g. [13] for the necessary background on Gröbner bases). This ideal coincides with $K[x,y,z]$ if and only if its reduced Gröbner basis consists of one nonzero

constant only. Hence, if the reduced Gröbner basis obtained consists of a nonzero constant, then we continue with Step 2. Otherwise we conclude that p is not a coordinate of $K[z][x,y]$.

Step 2. Working on $K(z)$ instead of $K[z]$, we apply the algorithm of Corollary 9.4.12 and determine whether p is a coordinate in $K(z)[x,y]$. If the answer is negative, then p cannot be a coordinate in $K[z][x,y]$. Otherwise p is a coordinate of $K[z][x,y]$. ■

9.4.3 New class of wild automorphisms

For $R = K, K(z), K[z]$, let $\mathrm{Aut}^0(R[x,y])$ be the group of augmentation-preserving automorphisms; i.e., $F = (f_1, f_2) \in \mathrm{Aut}^0(R[x,y])$ means that the polynomials f_1 and f_2 have no constant terms. Every automorphism G of $R[x,y]$ can be decomposed as $G = T(F)$, where $G = (x+a, y+b)$ for some $a, b \in R$ and $F = (f_1, f_2) \in \mathrm{Aut}^0(R[x,y])$. Hence, it is sufficient to study $\mathrm{Aut}^0(R[x,y])$ instead of $\mathrm{Aut}(R[x,y])$. By a result of Wright [404], the group $T^0(R[x,y])$ of tame automorphisms of $R[x,y]$ preserving the augmentation has a description similar to a free amalgamated product like $\mathrm{Aut}(K[x,y])$ does. In particular, $T^0(R[x,y])$ is generated by the elementary automorphisms

$$F = (x, y + f(x)), \quad G = (x + g(y), y),$$
$$f(x) \in R[x], \quad g(y) \in R[y], \quad f(0) = g(0) = 0,$$

and the diagonal automorphisms $D_{\alpha,\beta} = (\alpha x, \beta y)$, $\alpha, \beta \in R^*$. Since $D_{\alpha,\beta} = D_{\alpha\beta,1} \circ D_{\beta^{-1},\beta}$ and $D_{\beta^{-1},\beta}$ is a product of elementary linear automorphisms (because $\mathrm{SL}_2(R) = E_2(R)$), we obtain that every automorphism P in $T^0(R[x,y])$ has the form $P = H_1 \circ H_2 \circ \cdots \circ H_k \circ D_{\alpha,1}$, where each H_i is an elementary automorphism.

Every augmentation-preserving automorphism P of $K[z][x,y]$ can be considered as an automorphism in $\mathrm{Aut}^0(K(z)[x,y])$ and has a presentation $P = H_1 \circ H_2 \circ \cdots \circ H_k \circ D_{\alpha,1}$, where each H_i is an elementary automorphism of $K(z)[x,y]$ and $0 \neq \alpha \in K(z)$. The linear components of P and $H_1 \circ H_2 \circ \cdots \circ H_k$ are in $\mathrm{GL}_2(K[z])$ and $\mathrm{SL}_2(K(z))$, respectively. This easily implies that $\alpha \in K^*$ and both $D_{\alpha,1}$ and $H_1 \circ H_2 \circ \cdots \circ H_k$ are automorphisms of $K[z][x,y]$. This observation shows that, when studying automorphisms of $K[z][x,y]$, it is sufficient to consider automorphisms that are products of elementary automorphisms of $K(z)[x,y]$. We state the following natural problem.

Problem 9.4.17. Let T_k be the subgroup of $\mathrm{Aut}^0(K[z][x,y])$ generated by those automorphisms that can be presented as a product of not more than k elementary (and preserving the augmentation) automorphisms of $K(z)[x,y]$. Is it true that the sequence of subgroups

$$T_1 \subseteq T_2 \subseteq T_3 \subseteq \ldots$$

satisfies the ascending chain condition?

Obviously, every automorphism in $T^0(K[z][x,y])$ is a product of some $D_{\alpha,1}$ and an automorphism in T_1. More generally, every automorphism of $K[z][x,y]$ is a product of a $D_{\alpha,1}$ and an automorphism in T_k. Therefore, the minimal k with this property can serve as a measure of "how wild" the automorphism is.

Remark 9.4.18. It is easy to see that $T_1 = T_2$. Indeed, if $P = F \circ G \in T_2$, where

$$F = (x, y + f(x)), \quad G = (x + g(y), y), \quad f(x) \in K(z)[x], \quad g(y) \in K(z)[y],$$

then obviously

$$P = (x + g(y), y + f(x + g(y))) \in \operatorname{Aut} K[z][x,y],$$

which means that $g(y) \in K[z][y]$. Hence $F = P \circ G^{-1} \in \operatorname{Aut} K[z][x,y]$ and again we obtain that $f(x) \in K[z][x]$. Therefore, both F and G are tame automorphisms of $K[z][x,y]$ and $P \in T_1$; i.e., $T_1 = T_2$.

Example 9.4.19. By [288], the automorphism of Nagata

$$N = (x - 2(y^2 + zx)y - (y^2 + zx)^2 z, y + (y^2 + zx)z)$$

considered as an automorphism of $K(z)[x,y]$ has the presentation $N = G^{-1} \circ F \circ G$, where

$$F = (x, y + z^2 x), \quad G = \left(x + \frac{y^2}{z}, y\right).$$

Since $N \in T_3$ and the Nagata automorphism is wild when considered as an automorphism of $K[z][x,y]$, by Remark 9.4.18 we obtain that T_2 is a proper subgroup of T_3.

Now we start to study automorphisms in T_3 of the form $P = F^{-1} \circ G \circ F$, where $F = (x, y + f(x))$ and $G = (x + g(y), y)$ are elementary automorphisms of $K(z)[x,y]$. (Up to the order of variables, these automorphisms are "Nagata-like".) Since

$$P = (x + g(y + f(x)), y + f(x) - f(x + g(y + f(x)))),$$

we shall also describe the corresponding coordinate polynomials $x + g(y + f(x))$.

Lemma 9.4.20. *Let $f(x) \in K(z)[x]$, $g(y) \in K(z)[y]$ be such that $f(0) = g(0) = 0$ and $g(y + f(x)) \in K[z][x,y]$. Then $f(x)$ and $g(y)$ have presentations*

$$f(x) = \frac{a(x)}{b(z)}, \quad g(y) = d(b(z)y),$$

where $a(x) \in K[z][x]$, $d(y) \in K[z][y]$, $a(0) = d(0) = 0$, and $b(z) \in K[z]$.

Proof. We rewrite $f(x)$ in the form $f(x) = a(x)/b(z)$, where $a = a(x) \in K[z][x]$ (and $a(0) = 0$), $b(z) \in K[z]$, and $a(x) = a(x,z)$ and $b(z)$ are relatively prime in $K[x,z]$. In the formula

$$g(y+f(x)) = g\left(y + \frac{a(x)}{b(z)}\right) = \sum_{k=0}^{n} \frac{g^{(k)}(y)a^k(x)}{k!b^k(z)} \in K[z][x,y],$$

where $g^{(k)} = g^{(k)}(y)$ is the kth derivative of $g(y)$ (with respect to y), we replace x by 0 and obtain

$$g(y) = g(y+f(0)) \in K[z][y].$$

Hence

$$\sum_{k=1}^{n} \frac{g^{(k)}(y)a^k(x)}{k!b^k(z)} \in K[z][x,y],$$

$$a\left(\frac{g'b^{n-1}}{1!} + \frac{g''ab^{n-2}}{2!} + \cdots + \frac{g^{(n-1)}a^{n-2}b}{(n-1)!} + \frac{g^{(n)}a^{n-1}}{n!}\right) \equiv 0 \pmod{b^n},$$

and since a and b are relatively prime, we obtain that

$$\frac{g'b^{n-1}}{1!} + \frac{g''ab^{n-2}}{2!} + \cdots + \frac{g^{(n-1)}a^{n-2}b}{(n-1)!} + \frac{g^{(n)}a^{n-1}}{n!} \equiv 0 \pmod{b^n}.$$

Replacing x by 0, we obtain $g'b^{n-1} \equiv 0 \pmod{b^n}$, and hence $g' \equiv 0 \pmod{b}$, and the coefficient of y^k in $g(y)$ is divisible by $b(z)$ for $k \geq 1$. Let $g'(y) = b(z)g_1(y)$ for some $g_1(y) \in K[z][y]$. Now our congruence has the form

$$a\left(\frac{g_1'b^{n-2}}{2!} + \frac{g_1''ab^{n-3}}{3!} + \cdots + \frac{g_1^{(n-2)}a^{n-3}b}{(n-1)!} + \frac{g_1^{(n-1)}a^{n-2}}{n!}\right) \equiv 0 \pmod{b^{n-1}}.$$

Again, the coefficient of y^k in $g_1(y)$ is divisible by $b(z)$ for $k \geq 1$, and hence the coefficient of y^{k+1} in $g(y)$ is divisible by $b^2(z)$ for any $k \geq 1$. Continuing in this way, we obtain that the coefficient of g^k in $g(y)$ is divisible by $b^k(z)$ for all k; i.e., $g(y) = d(b(z)y)$ for some $d(y) \in K[z][y]$. ∎

Lemma 9.4.21. *Let $a(x) \in K[z][x]$, $d(y) \in K[z][y]$, $b(z) \in K[z]$, $a(0) = d(0) = 0$, and let $a(x) = a(x,z)$ and $b(z)$ be relatively prime in $K[x,z]$. If the polynomial $a(x + d(a(x) + b(z)y)) - a(x)$ is divisible by $b(z)$, then the polynomial $d(y)$ is also divisible by $b(z)$.*

Proof. Let $b(z) = \prod_{i=1}^{s} b_i^{p_i}(z)$, where $b_1(z), \ldots, b_s(z)$ are the different irreducible factors of $b(z)$. It is sufficient to show that $d(y)$ is divisible by all polynomials $b_i^{p_i} = b_i^{p_i}(z)$. Since $b_i^{p_i}$ divides the polynomial $a(x + d(a(x) + b(z)y)) - a(x)$, it divides also $a(x + d(a(x))) - a(x)$. We want to show that the polynomial $d(y)$ is also divisible by $b_i^{p_i}$, assuming

that $a(x)$ is relatively prime with b_i. Working modulo $b_i^{p_i}$, we obtain

$$0 \equiv a(x+d(a(x))) - a(x) \equiv \sum_{k=1}^{n} \frac{a^{(k)}(x)}{k!} d^k(a(x)) \pmod{b_i^{p_i}}.$$

Let $a(x) \equiv x^q a_1(x) \pmod{b_i}$, $a_1(x) \in K[z][x]$, and let q be the maximal integer with this property; i.e., $a_1(0) \not\equiv 0 \pmod{b_i}$. Since $a(0) = 0$, we have that $q \geq 1$. Let us first assume that $d(y)$ is not divisible by b_i. Let r be the maximal integer with $d(y) \equiv y^r d_1(x) \pmod{b_i}$, $d_1(y) \in K[z][y]$, $d_1(0) \not\equiv 0 \pmod{b_i}$. Again, $r \geq 1$. For $k \leq q$, the derivative $a^{(k)}(x)$ has the form $a^{(k)}(x) \equiv x^{q-k} c_k(x) \pmod{b_i}$, $c_k(x) \in K[z][x]$, $c_k(0) \not\equiv 0 \pmod{b_i}$. Hence

$$\begin{aligned} &a^{(k)}(x) d^k(a(x)) \\ &\quad \equiv x^{q-k} c_k(x) ((x^q a_1(x))^r d_1(x^q a_1(x)))^k \equiv x^{q-k+kqr} e_k(x) \pmod{b_i}, \end{aligned}$$

where $e_k(x) \in K[z][x]$ and $e_k(0) \not\equiv 0 \pmod{b_i}$. For $k > q$, we have that

$$a^{(k)}(x) d^k(a(x)) \equiv a^{(k)}((x^q a_1(x))^r d_1(x^q a_1(x)))^k \pmod{b_i},$$

and $a^{(k)}(x) d^k(a(x))$ is divisible by x^{kqr} modulo b_i. If $qr > 1$, then the degrees t_k of x^{t_k} dividing $a^{(k)}(x) d^k(a(x))$ modulo b_i satisfy the inequalities

$$t_1 = q-1+qr < t_2 = q-2+2qr < \cdots < t_q = q^2 r < (q+1)qr \leq t_{q+1}, \ldots, t_n.$$

Hence $a(x+d(a(x))) - a(x) \equiv x^{q-1+qr} a_0(x) \pmod{b_i}$, $a_0(x) \in K[z][x]$, and $a_0(0) \equiv e_1(0) \not\equiv 0 \pmod{b_i}$. But this contradicts the assumption that $a(x+d(a(x))) - a(x) \equiv 0 \pmod{b_i}$. The case $qr = 1$ (i.e., $q = r = 1$) is similar. Again $a'(x) d(a(x)) \equiv x c_1(x) \pmod{b_i}$ with $c_1 \in K[z][x]$, $c_1(0) \not\equiv 0 \pmod{b_1}$, and $a^{(k)}(x) d^k(a(x))$ is divisible by x^2 modulo b_i for $k > 1$. Again $a(x+d(a(x))) - a(x) \equiv x a_0(x) \pmod{b_i}$, $a_0(x) \in K[z][x]$, and $a_0(0) \equiv e_1(0) \not\equiv 0 \pmod{b_i}$, which is a contradiction. Hence, in all cases we have that b_i divides $d(y)$. Let $d(y) = b_i^t d_0(y)$, where $t \geq 1$ and $d_0(y) \in K[z][y]$ is relatively prime with b_i. Then the congruence

$$\sum_{k=1}^{n} \frac{a^{(k)}(x)}{k!} d^k(a(x)) \equiv 0 \pmod{b_i^{p_i}}$$

has the form

$$\sum_{k=1}^{n} \frac{a^{(k)}(x)}{k!} d_0^k(a(x)) b_i^{kt} \equiv 0 \pmod{b_i^{p_i}}$$

and, if $t < p_i$, we obtain $a'(x) d_0(a(x)) \equiv 0 \pmod{b_i}$. Since $a(x)$ is relatively prime with b_i and $a(0) = 0$, we obtain that $a'(x)$ is also relatively prime with b_i and, hence, b_i divides $d_0(a(x))$. But, as above, we see that this is impossible. Therefore $t \geq p_i$ and $b_i^{p_i}$ divides $d(x)$. Hence b also divides $d(y)$. ■

A derivation δ is called *triangular* if $\delta(x_i) \in K[x_{i+1}, \ldots, x_n]$, $i = 1, \ldots, n$. Clearly, every triangular derivation is locally nilpotent. For every locally nilpotent derivation δ and for any element w in the kernel of δ, the mapping of $K[X]$

$$\exp(w\delta) = \sum_{n \geq 0} \frac{w^n \delta^n}{n!}$$

is a well-defined automorphism of $K[X]$.

Recall that $F = (f_1, \ldots, f_n)$ of $K[x_1, \ldots, x_n]$ is a *stably tame* automorphism if its extension $(f_1, \ldots, f_n, x_{n+1}, \ldots, x_{n+m})$ to an automorphism of $K[x_1, \ldots, x_{n+m}]$ for some $m > 0$ is a tame automorphism of $K[x_1, \ldots, x_{n+m}]$. Similarly, one can define stably tame automorphisms of $R[x_1, \ldots, x_n]$ for any commutative algebra R.

The next result describes the tame and the wild automorphisms of the form $P = F^{-1} \circ G \circ F \in T_3$, where $F = (x, y + f(x))$ and $G = (x + g(y), y)$ are elementary automorphisms of $K(z)[x, y]$, and shows that all automorphisms of this form are stably tame; i.e., they are really "Nagata-like". Also, it turns out that these automorphisms are like those considered in Example 9.4.15.

Theorem 9.4.22. *Let $0 \neq f(x) \in K(z)[x]$, $0 \neq g(y) \in K(z)[y]$, where $f(0) = g(0) = 0$ and $f(x) = a(x)/b(z)$, $a(x) \in K[z][x]$, $b(z) \in K[z]$, the polynomials a and b being relatively prime in $K[x, z]$. Define the automorphisms F and G of $K(z)[x, y]$ by*

$$F = (x, y + f(x)), \quad G = (x + g(y), y).$$

(i) *The composition $P = F^{-1} \circ G \circ F$ is an automorphism of $K[z][x, y]$ if and only if $g(y) = b(z)q(b(z)y)$ for some $q(y) \in K[z][y]$. In this case, P is equal to the automorphism $\exp(w\delta)$, where δ is the triangular derivation of $K[z][x, y]$ defined by*

$$\delta(x) = b(z), \quad \delta(y) = -a'(x)$$

and $w = q(a(x) + b(z)y)$ is in the kernel of δ.

(ii) *Let $P = F^{-1} \circ G \circ F$ be an automorphism of $K[z][x, y]$. Then P is wild (as an automorphism of $K[z][x, y]$) if and only if the coefficient of x^k in $f(x)$ is not in $K[z]$ for some $k > 1$.*

(iii) *If $P = F^{-1} \circ G \circ F \in \operatorname{Aut} K[z][x, y]$, then P is stably tame and becomes tame as an automorphism of $K[z][x, y, t]$ (acting identically on t).*

Proof.

(i) Direct computations show that

$$P = (p_1, p_2) = (x + g(y + f(x)), y + f(x) - f(x + g(y + f(x)))).$$

If P is an automorphism of $K[z][x,y]$, then $p_1, p_2 \in K[z][x,y]$. Applying Lemma 9.4.20 to p_1, we obtain that $g(y) = d(b(z)y)$ for some $d(y) \in K[z][y]$ and $b(z) \in K[z]$. Now Lemma 9.4.21 gives $d(y) = b(z)q(y)$, $q(y) \in K[z][y]$.

Now let $g(y) = b(z)q(b(z)y)$ for some $q(y) \in K[z][y]$. We define the derivation δ of $K[z][x,y]$ by $\delta(x) = b(z)$, $\delta(y) = -a'(x)$. Clearly, δ is triangular. It is easy to verify that $w = q(a(x) + b(z)y)$ is in the kernel of δ. Hence $\exp(w\delta)$ is an automorphism of $K[z][x,y]$ and we have to show that P and $\exp(w\delta)$ are equal on the generators x and y of $K[z][x,y]$. Again, direct calculations show that

$$\begin{aligned}
\exp(w\delta)(x) &= x + w\delta x = x + bq(a(x) + by) = p_1,\\
\exp(w\delta)(y) &= y + \sum_{k\geq 1} \frac{w^k \delta^k y}{k!} = y - \frac{1}{b}\sum_{k\geq 1} \frac{a^{(k)}(x) b^k q^k (a(x) + by)}{k!}\\
&= y + \frac{1}{b}(a(x) - a(x + bq(a(x) + by)) = p_2.
\end{aligned}$$

(ii) Since $P \in \mathrm{Aut}(K[z][x,y])$, by (i) we obtain that $g(y) = b(z)q(b(z)y)$ for some $q(y) \in K[z][y]$ and

$$P = \left(x + bq(a(x) + by), y + \frac{1}{b}(a(x) - a(x + bq(a(x) + by)))\right).$$

Hence $x + bq(a(x) + by)$ is a coordinate of $K[z][x,y]$. If the coefficient of x^k in $f(x)$ is not in $K[z]$ for some $k > 1$, this means that the coefficient of x^{k-1} of $a_x(x,z)$ is not divisible by $b(z)$, and Example 9.4.15 shows that P is a wild automorphism of $K[z][x,y]$. Now, let the coefficients of x^k in $f(x)$ be in $K[z]$ for all $k > 1$; i.e., $f(x) = c(z)/b(z)x + x^2 f_0(x,z)$, where $c(z)$ and $b(z)$ are relatively prime in $K[z]$ and $f_0(x,z) \in K[x,z]$. If $Q = (x, y - x^2 f_0(x,z))$, then the automorphism P is tame if and only if $P_1 = Q^{-1} \circ P \circ Q = F_1^{-1} \circ G \circ F_1$ is tame, where $F_1 = (x, y + c(z)x/b(z))$. In this case, P_1 is equal to $\exp(w\delta)$, where $w = q(c(z)x + b(z)y)$ and the derivation δ satisfies $\delta(x) = b(z)$, $\delta(y) = -c(z)$. Since $b(z)$ and $c(z)$ are relatively prime in $K[z]$, there exist $b'(z), c'(z) \in K[z]$ such that $b'c - c'b = 1$; i.e., the endomorphism

$$S = (x_1, y_1) = (cx + by, c'x + b'y)$$

of $K[z][x,y]$ is a linear (and hence tame) automorphism. Now we calculate P_1 with respect to the generators x_1, y_1:

$$\begin{gathered}
\delta(x_1) = 0, \quad \delta(y_1) = c'b - b'c = -1, \quad w = q(x_1),\\
P_1(S) = P_1(x_1, y_1) = (\exp(w\delta)(x_1), \exp(w\delta)(y_1)) = (x_1, y_1 - q(x_1)).
\end{gathered}$$

Since P_1 is elementary with respect to the tame system of generators x_1, y_1, we obtain that P_1 and hence P are tame.

(iii) The statement follows immediately from the proof of the result of M. Smith [370] that for any triangular derivation δ of $K[X] = K[x_1, \ldots, x_n]$ and any $w \in \mathrm{Ker}\,\delta$, the automorphism $\exp(w\delta)$ is stably tame. If we extend

our δ to a derivation of $K[z][x,y,t]$ by $\delta(t) = 0$, we obtain that $w = q(a(x) + by)$ is still, in the kernel of δ,

$$\exp(w\delta)(x,y,t) = (p_1, p_2, t) = Q^{-1} \circ E \circ Q \circ E^{-1},$$

where $Q = (x, y, t+w)$, $E = \exp(t\delta)$, and Q and E are tame automorphisms of $K[z][x,y,t]$. ■

Remark 9.4.23. Wright [404, in the proof of the corollary to Theorem 5, p. 247] gave a family of wild automorphisms of $R[x,y]$, where R is a principal ideal domain. For $R = K[z]$ his automorphisms are given by

$$P = \left(x + b^3 \left(y + \frac{x^2}{b} \right)^2, y + \frac{x^2}{b} - \frac{1}{b} \left(x + b^3 \left(y + \frac{x^2}{b} \right)^2 \right)^2 \right),$$

where $b = b(z) \in K[z]$ is not a constant. All these automorphisms can be obtained from Theorem 9.4.22 for

$$f(x) = \frac{x^2}{b}, \quad g(y) = b(by)^2.$$

Theorem 9.4.22 (iii) has the following generalization, which is obtained by multiple applications of the idea of M. Smith [370] and gives new stably tame automorphisms. Note that for $A = (y, x)$ and the triangular automorphism $F = (x, y + f(x))$, we have $A^{-1} = A$, and the conjugate $A \circ F \circ A$ is equal to the automorphism $(x + f(y), y)$, which is triangular with respect to another ordering of the variables.

Theorem 9.4.24. *Let $a_i \in K[x,z]$, $b_i \in K[z]$, $f_i = a_i/b_i$, $i = 1, \ldots, k$, $q \in K[y,z]$ be any polynomials, and let $A = (y, x)$, $F_i = (x, y + f_i(x))$, $i = 1, \ldots, k$, be automorphisms of $K(z)[x,y]$. Then there exist sufficiently large positive integers $m_1, \ldots, m_k$ such that for $G = (x + b_1^{m_1} \ldots b_k^{m_k} q(y), y)$ the mapping*

$$P = F_k^{-1} \circ A \circ F_{k-1}^{-1} \circ A \circ \cdots \circ F_1^{-1} \circ G \circ F_1 \circ A \circ \cdots \circ F_{k-1} \circ A \circ F_k$$

is a stably tame automorphism of $K[z][x,y]$.

Proof. Let $q(t) = \sum_{j=0}^{n} c_j(z) y^j$ for some polynomials $c_j \in K[z]$. Let r_i, s_i, $i = 1, \ldots, k$, be positive integers, and let $m_i = r_i + (n+1)s_i$. Clearly,

$$b_1^{m_1} q(y) = b_1^{s_1} \sum_{j=0}^{n} (c_j b_1^{r_1 + (n-j)s_1})(b_1^{s_1} y)^j = b_1^{s_1} q_1(b_1^{s_1} y),$$

where $q_1(y) = \sum_{j=0}^{n} c_j b_1^{r_1 + (n-j)s_1} y^j \in K[z][y]$. Similarly, we obtain that

$$b_1^{m_1} \ldots b_k^{m_k} q(y) = b_1^{s_1} \ldots b_k^{s_k} q_k(b_1^{s_1} \ldots b_k^{s_k} y)$$

for some $q_k \in K[z][y]$. As in the proof of Theorem 9.4.22 (iii), for $k = 1$ we fix $s_1 = 1$ and obtain that

$$F_1^{-1} \circ G \circ F_1 = \exp(w\delta),$$

where $\delta = b_2^{s_2} \dots b_k^{s_k} \delta_0$, $\delta_0(x) = -b_1$, $\delta_0(y) = (a_1)_x$,

$$w = b_2^{s_2} \dots b_k^{s_k} q_k(b_2^{s_2} \dots b_k^{s_k}(a(x) + b_1 y)) \in \operatorname{Ker} \delta,$$

and, after extending the action to $K[z][x,y,t_1]$, the automorphism $F_1^{-1} \circ G \circ F_1$ is expressed in terms of triangular automorphisms

$$\exp(b_2^{s_2} \dots b_k^{s_k} t_1 \delta_0), \quad (x, y, z, t_1 + b_2^{s_2} \dots b_k^{s_k} q_k(b_2^{s_2} \dots b_k^{s_k}(a(x) + b_1 y))),$$

and their inverses. Continuing in this way, we obtain that the automorphism $A \circ F_{k-1}^{-1} \circ \dots \circ G \circ \dots \circ F_{k-1} \circ A$ becomes tame in $K[z][X]$ for $X = \{x_1, \dots, x_{k+1}\} = \{x, y, t_1, \dots, t_{k-1}\}$ and is a composition of automorphisms of the type

$$G_i = (x_1 + b_k^{s_k} u_i(x_2, \dots, x_{k+1}), x_2, \dots, x_{k+1})$$

for some polynomials $u_i \in K[z][x_2, \dots, x_{k+1}]$ up to a permutation of variables. Hence we have to show that $F_k^{-1} \circ G_i \circ F_k$ is an automorphism of $K[z][x_1, \dots, x_{k+1}]$ that becomes stably tame in $K[z][x_1, \dots, x_{k+2}]$, where s_k is big enough and F_k is one of the following types (again, up to a permutation of variables):

$$F_k = (x_1 + a_k(x_2)/b_k, x_2, \dots, x_{k+2}),$$
$$F_k = (x_1, x_2 + a_k(x_3)/b_k, x_3, \dots, x_{k+2}),$$
$$F_k = (x_1, x_2 + a_k(x_1)/b_k, x_3, \dots, x_{k+2}).$$

Straightforward calculations show that in the first two cases the composition $F_k^{-1} \circ G_i \circ F_k$ is triangular for s_k sufficiently large and hence tame. In the third case, we may consider $F_k^{-1} \circ G_i \circ F_k$ as an automorphism of $K(x_3, \dots, x_{k+1})[z][x_1, x_2]$ that keeps $K[x_3, \dots, x_{k+1}, z][x_1, x_2]$ invariant. As for $k = 1$, we obtain that $F_k^{-1} \circ G_i \circ F_k$ is a composition of tame automorphisms of $K[x_3, \dots, x_{k+1}, z][x_1, x_2, x_{k+2}]$, and this completes the proof. ■

Theorem 9.4.22 shows that the polynomials

$$p(x,y) = x + bq(a(x) + by), \quad a(x) \in K[z][x], \quad b(z) \in K[z], \quad q(u) \in K[z][u]$$

are images of x under automorphisms of $K[z][x,y]$ of a very special form. Now we are interested in more general polynomials than those considered in Example 9.4.15. We study polynomials of the form

$$p(x,y) = x + d(a(x) + by),$$

where $a(x) \in K[z][x]$, $b(z) \in K[z]$, $d(u) \in K[z][u]$, and $a(0) = d(0) = 0$. If $e(z) \in K[z]$ is a divisor of $b(z)$ and $a(x)$, we may replace $a(x)$ with $a_1(x) = a(x)/e(z)$, $b(z)$ with $b_1(z) = b(z)/e(z)$, $d(u)$ with $d_1(u) = d(e(z)u)$, and without loss of generality we may assume that $a(x)$ and $b(z)$ are relatively prime in $K[x,z]$. Besides, if $p(x,y) \in K[z][x,y]$ is a coordinate polynomial, then it has a unimodular gradient with respect to x and y. In our case this

means that

$$p_x = 1 + a_x(x)d_u(a(x) + by), \quad p_y = bd_u(a(x) + by)$$

generate $K[z][x, y]$ as an ideal. By Hilbert's Nullstellensatz, this is equivalent to the statement that $p_x = p_x(x, y, z)$ and $p_y = p_y(x, y, z)$ have no common zeros (x_0, y_0, z_0) in the algebraic closure of K. Since $a(x, z)$ and $b(z)$ are relatively prime and $a(0, z) = 0$, we obtain that $a_x(x)$ is also relatively prime with $b(z)$. If z_0 is a zero of $b(z)$, and $d(u) = d(u, z)$ does not vanish for $z = z_0$, we derive that $p_x(x, y, z_0) = 1 + a_x(x, z_0)d_u(a(x, z_0))$ is a nonzero polynomial of x. The only case where p_x and p_y have no common zeros is where this polynomial is a constant; i.e., $d(u)$ has the form $d(u) = e(z)u + b_0(z)u^2d_1(u)$, where $e(z) \in K[z]$ is relatively prime with $b(z)$ and $b_0(z)$ is the product of all irreducible components of $b(z)$. Hence, with this exception only, we may assume that the polynomial $d(u)$ is divisible by $b_0(z)$; i.e., it is of the form considered in Example 9.4.15. By finding an automorphism that sends x to $p(x, y)$, we also shed some light on automorphisms of $K[z][x, y]$ that are products of three elementary automorphisms of $K(z)[x, y]$.

Lemma 9.4.25. *Let $P = (p_1, p_2)$ be an automorphism of $K(z)[x, y]$ such that $p_1, p_2 \in K[z][x, y]$. Then P is an automorphism of $K[z][x, y]$ if its Jacobian matrix is invertible in $\mathrm{GL}_2(K[z][x, y])$.*

Proof. We make use of the Keller theorem (see [173] or [39]): If P is an endomorphism of $K[X]$ that induces an automorphism of $K(X)$ and the Jacobian matrix J_P of P is invertible in $\mathrm{GL}_n(K[X])$, then P is an automorphism of $K[X]$. In our case, since P fixes z, the determinant of the Jacobian matrix of P considered as an endomorphism of $K[x, y, z]$ coincides with the determinant of the Jacobian matrix considering P as an endomorphism of $K[z][x, y]$. The proof is completed by the Keller theorem because P induces an automorphism of $K(x, y, z)$. ■

Theorem 9.4.26. *Let $0 \neq a(x) = a(x, z) \in K[z][x]$, $0 \neq q(u) = q(u, z) \in K[z][u]$, $a(0) = q(0) = 0$, $0 \neq b(z) \in K[z]$, and let $a(x, z)$, $b(z)$ be relatively prime in $K[x, z]$. Let $b_0(z)$ be the product of all irreducible factors of $b(z)$. Then the polynomial*

$$p(x, y) = x + b_0q(a(x) + by) = x + b_0(z)q(a(x, z) + b(z)y, z)$$

is an image of x under an automorphism of $K[z][x, y]$ that is a product of three elementary automorphisms of $K(z)[x, y]$. Moreover, $p(x, y)$ is a wild coordinate if $b(z)$ does not divide the coefficient of x^i in $a_x(x)$ for some $i > 0$.

Proof. We shall find a polynomial $c(v) \in K[z][v]$, $c(0) = 0$, such that $P = F_2 \circ G \circ F_1 = (p, r)$ is an automorphism of $K[z][x, y]$ for some $r \in K[z][x, y]$,

where

$$F_1 = \left(x, y + \frac{a(x)}{b}\right), \quad F_2 = \left(x, y + \frac{c(x)}{b}\right), \quad G = (x + b_0 q(by), y)$$

are automorphisms of $K(z)[x,y]$. Direct calculations show that

$$\begin{aligned} P &= (p(x,y), r(x,y)) \\ &= \left(x + b_0 q(a(x) + by), y + \frac{1}{b}\left(a(x) + c(x + b_0 q(a(x) + by))\right)\right) \end{aligned}$$

and the Jacobian matrix of P is equal to

$$J_P = \begin{pmatrix} 1 + b_0 q_u a_x & b_0 q_u b \\ \frac{1}{b}(a_x + c_v(1 + b_0 q_u a_x)) & 1 + c_v b_0 q_u \end{pmatrix},$$

where $a_x = a_x(x)$, $q_u = q_u(a(x)+by)$, $c_v = c_v(x+b_0 q(a(x)+by))$. It is easy to see that the determinant of $J(\varphi)$ is equal to 1. By Lemma 9.4.25, the proof of the theorem will be completed if we show that $r(x,y) \in K[z][x,y]$ for some $c(v) \in K[z][v]$. Clearly, $r(x,y)$ is in $K[z][x,y]$ if and only if

$$a(x) + c(x + b_0(z) q(a(x) + b(z)y)) \equiv 0 \pmod{b(z)}.$$

This is equivalent to $a(x) + c(x + b_0(z) q(a(x))) \equiv 0 \pmod{b(z)}$. Since $b(z)$ is a divisor of $b_0^n(z)$ for some n, it is sufficient to show that the congruence

$$a(x) + c(x + b_0(z) q(a(x))) \equiv 0 \pmod{b_0^n(z)}$$

has a solution $c(v) \in K[z][v]$ for every $n > 0$. Clearly, the congruence has a solution $c_1(v) \equiv -a(v) \pmod{b_0(z)}$. Let us assume that we have found a solution $c_m(v)$ modulo $b_0^m(z)$. Then, writing $c(v)$ in the form $c(v) = c_m(v) + b_0^m(z) d(v)$, we see that the congruence

$$a(x) + c_m(x + b_0(z) q(a(x))) + b_0^m(z) d(x + b_0(z) q(a(x))) \equiv 0 \pmod{b_0^{m+1}(z)}$$

has a solution $d(v) \in K[z][v]$, namely

$$d(v) \equiv -\frac{1}{b_0^m(z)}(a(v) + c_m(v + b_0(z) q(a(v)))) \pmod{b_0(z)}.$$

■

Remark 9.4.27. The proof of Theorem 9.4.26 gives a description of the generators of the group T_3 defined in Problem 9.4.17. It is generated by all elementary automorphisms of $K[z][x,y]$ and the automorphisms P defined by

$$P = (p, r) = \left(x + q(a(x) + b(z)y), y + \frac{a(x)}{b(z)} + \frac{1}{d(z)} c(x + q(a(x) + b(z)y))\right),$$

where $a(x), b(z), c(v), d(z), q(u)$ are nonzero polynomials, $a(x) \in K[z][x]$, $b(z), d(z) \in K[z]$, $c(v) \in K[z][v]$, $q(u) \in K[z][u]$, $a(0) = c(0) = q(0) = 0$, such that $r \in K[z][x,y]$. The careful study of the proof of Theorem 9.4.26

gives that it is sufficient to choose in the set of generators of T_3 only one P for each coordinate polynomial r; i.e., by fixing r, we also fix $c(v)$ and $d(z)$.

All known stably tame automorphisms of $K[X]$ can be obtained by the method of M. Smith [370] and are exponential automorphisms of locally nilpotent derivations; see [104]. The automorphisms of Theorem 9.4.22 and 9.4.24 are also of this kind. We do not know whether the automorphisms involved in Theorem 9.4.26 can be obtained as compositions (considered as automorphisms of $K[z][x,y]$) of stably tame exponential automorphisms of locally nilpotent derivations.

Problem 9.4.28.

(i) Are all automorphisms in the group $T_3 \subset \operatorname{Aut} K[z][x,y]$ stably tame?

(ii) Are all automorphisms of $K[z][x,y]$ stably tame?

10

Test Elements of Polynomial and Free Associative Algebras

Let K be a field of any characteristic, and let $K[X] = K[x_1, \ldots, x_n]$ and $K\langle X\rangle = K\langle x_1, \ldots, x_n\rangle$ be respectively the polynomial and the free associative algebra freely generated by a set $X = \{x_1, \ldots, x_n\}$. The general problem under discussion in this chapter is how to recognize automorphisms of $K[X]$ and $K\langle X\rangle$. Following van den Essen and Shpilrain [124], we give the following definitions.

Definition 10.0.1. A polynomial $p = p(X)$ from $K[X]$ is a test polynomial if for every n-tuple $F \in (K[X])^n$ the equality $p(F) = p(X)$ implies that the map $X \to F$ induces an automorphism of $K[X]$.

A polynomial $p = p(X)$ is a test polynomial in a class $\mathcal{S}$ of polynomial mappings of $K[X]$ if, for any $\varphi \in \mathcal{S}$, $\varphi(p) = p$ implies that φ is an automorphism of $K[X]$.

Definition 10.0.2. Let S be a class of endomorphisms of $K[X]$ (or $K\langle X\rangle$), and let M be a subclass of S. We call a polynomial $p(X) = p(x_1, \ldots, x_n)$ a *test polynomial for M in S* if for any $F \in S$ the equality $p(F) = p(X)$ implies $F \in M$. If a test polynomial p is fixed by an automorphism F, we say that p *recognizes* F.

Test elements of $K\langle X\rangle$ are defined similarly.

Definition 10.0.3. The *outer rank* of a polynomial $p(X)$ in $K[X]$ (or an element of $K\langle X\rangle$) is the minimum number of generators x_i on which an automorphic image of p can depend.

Van den Essen and Shpilrain [124] proved that any test polynomial $p(X)$ is of maximum outer rank n.

The main purpose of this chapter is to construct test elements for $K[X]$ and $K\langle X\rangle$. This problem has been considered for various algebraic systems. Dicks [93], using the description of Aut $K\langle x_1, x_2\rangle$ given by Makar-Limanov [233] and Czerniakiewicz [86], has established that an endomorphism $F = (f_1, f_2)$ of the free algebra $K\langle x_1, x_2\rangle$ is an automorphism if and only if $[f_1, f_2] = \alpha[x_1, x_2]$ for some nonzero element α from K. Therefore the commutator $[x_1, x_2] = x_1x_2 - x_2x_1$ is a test element for $K\langle x_1, x_2\rangle$.

It seems to be very difficult to classify all test elements (or even test elements in the class of monomorphisms) of polynomial and free associative algebras. In fact, the only previously known test elements were the commutator $[x_1, x_2]$ for $K\langle x_1, x_2\rangle$ [93] and $x_1^2 + \cdots + x_n^2$ for the polynomial algebra $\mathbb{R}[X]$ given in [124]. On the other hand, it was shown in [108] that the exponential automorphisms of $K[X]$ have no test polynomials. If ∂ is a locally nilpotent derivation of $K[X]$, char $K = 0$, and $p(X) \in K[X]$ is fixed by the automorphism $\exp \partial$, then there are monomorphisms of $K[X]$ that are not automorphisms and also fix $p(X)$.

Jelonek [163] showed that a generic polynomial of degree $> n$ in $\mathbb{C}[x_1, \ldots, x_n]$ is a test polynomial for monomorphisms. The statement "a generic polynomial of degree d has a property W" means that there exists a Zariski open dense subset $U \subseteq \mathcal{H}_d$ of the set $\mathcal{H}_d$ of all polynomials of degree d such that every element of U has the property W.

In this chapter, we construct families of test elements for both polynomial algebras and free associative algebras.

The chapter is organized as follows. In Section 10.1, we give a family of test polynomials for the polynomial algebra $K[x_1, \ldots, x_n]$. In Section 10.2, several families of test polynomials for the free algebra $K\langle x_1, \ldots, x_n\rangle$ are constructed. In the concluding Section 10.3, we propose some open problems related to test polynomials.

First we have to recall some terminology and notation. Every map $X \to K[X]$ can be extended to an endomorphism of $K[X]$. If $x_i \to f_i$, $i = 1, \ldots, n$, we denote the corresponding map and the induced endomorphism by $F = (f_1, \ldots, f_n)$. In particular, we use the notation $p(X)$ for a polynomial $p(x_1, \ldots, x_n)$ and $p(F)$ for $p(f_1, \ldots, f_n)$. If F is an automorphism, we call the polynomials f_i *coordinate polynomials*. We use similar notation for the maps $X \to K\langle X\rangle$, except we call f_i *primitive elements*. Recall that an automorphism F is *affine* if $F = (\alpha_1 + g_1, \ldots, \alpha_n + g_n)$, where $\alpha_i \in K$ and $G = (g_1, \ldots, g_n)$ is an invertible linear transformation. *Triangular* automorphisms are of the form $F = (f_1, \ldots, f_n)$, where $f_i = \alpha_i x_i + h_i$, $0 \neq \alpha_i \in K$, and the polynomials h_i do not depend on $x_1, \ldots, x_i$.

Let $Y = \{y_1, \ldots, y_n\}$ be another set of free generators of $K[X]$ (or of $K\langle X\rangle$), and let the polynomial $p(X) \in K[X]$ be written as $q(Y) = p(X)$.

If for any choice of $Y \in \operatorname{Aut} K[X]$ the polynomial $q(Y)$ depends essentially on each variable y_i, we call $p(X)$ a *polynomial of maximal rank.*

Remark 10.0.4. Let $F = (\alpha_1 + g_1, \ldots, \alpha_n + g_n)$ be an endomorphism of $K[X]$ (or of $K\langle X\rangle$), where $\alpha_i \in K$ and the polynomials g_i have no constant terms, $i = 1, \ldots, n$. Let $H = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. Then the composition of F and H is $F \circ H = G = (g_1, \ldots, g_n)$, and F is an automorphism if and only if $F \circ H$ is an automorphism. From this point of view, it is sufficient to consider test polynomials in the class of all endomorphisms $G = (g_1, \ldots, g_n)$ without constant terms of the polynomials g_i. We call such endomorphisms *endomorphisms without constant terms.*

Remark 10.0.5. Let F and H be automorphisms of $K[X]$ (or of $K\langle X\rangle$). If $p(X)$ is a test polynomial recognizing F, then $p(H)$ is a test polynomial recognizing $G = H^{-1}(F(H))$. (In this equality, we consider G and H as elements in $(K[X])^n$ or $(K\langle X\rangle)^n$, not the induced automorphisms.) Clearly, since $\operatorname{End}(K[X]) \circ H = \operatorname{End}(K[X])$, we obtain that $q(X) = p(H)$ is also a test polynomial and

$$p(H)(G) = p(H(G)) = p(F(H)) = p(H).$$

Hence $p(H)$ is a test polynomial recognizing $G = H^{-1}(F(H))$. Obviously, a similar statement holds for the test polynomials if we restrict our considerations to automorphisms and endomorphisms without constant terms.

Lemma 10.0.6. *If the homogeneous component of minimal degree of the polynomial $p(X)$ from $K[X]$ (or from $K\langle X\rangle$) is of maximal rank, then $p(X)$ is a test polynomial for injective endomorphisms in the class of all endomorphisms without constant terms.*

Proof. Let $p_k(X)$ be the homogeneous component of minimal degree of $p(X)$, and let $F = (f_1, \ldots, f_n)$ be an endomorphism from the class under consideration. Let $G = (g_1, \ldots, g_n)$ be the linear component of F. If $p(F) = p(X)$, we obtain that the homogeneous component of minimal degree of $p(F)$ is $p_k(G) = p_k(X)$. If $g_1, \ldots, g_k$ are linearly dependent, then they are linear combinations of $y_1, \ldots, y_{n-1}$ for a system of free generators $y_1, \ldots, y_n$ obtained from $x_1, \ldots, x_n$ by a linear transformation. This contradicts the maximal rank of $p_k(X)$. Hence $g_1, \ldots, g_n$ are linearly independent, and this implies that the endomorphism F is injective. ■

10.1 Test Polynomials in Polynomial Algebras

In this section, we assume that the ground field K is of characteristic zero and consider endomorphisms of $K[X] = K[x_1, \ldots, x_n]$. We start with some "negative" results and examples. The following example shows that the properties of the ground field are essential for test polynomials.

Example 10.1.1. If the field K of characteristic zero contains $\sqrt{-1}$, then the polynomial

$$p(X) = x_1^2 + \cdots + x_n^2, \quad n \geq 2,$$

is not a test polynomial for automorphisms of $K[X]$ in the class of all endomorphisms. Indeed, let

$$F = \left(\frac{1}{2}(1 + x_1^2 + x_2^2), \frac{\sqrt{-1}}{2}(-1 + x_1^2 + x_2^2), x_3, \ldots, x_n\right).$$

Obviously F is not invertible because its image does not contain monomials of odd degree with respect to x_1 and x_2. Easy calculations show that $p(F) = p(X)$; i.e., $p(X)$ is not a test polynomial. As we have mentioned before, $p(X)$ is the only known test polynomial for $\mathbb{R}[X]$.

Example 10.1.2. Consider the Nagata automorphism [288]

$$N = (x_1 - 2x_2(x_2^2 + x_1x_3) - x_3(x_2^2 + x_1x_3)^2, x_2 + x_3(x_2^2 + x_1x_3), x_3).$$

It fixes $q(X) = x_2^2 + x_1x_3$. For every polynomial $u \in K[x_1, x_2, x_3]$, the endomorphism

$$U = (x_1 - 2x_2u - x_3u^2, x_2 + x_3u, x_3)$$

also fixes $q(X)$. Clearly, u may be chosen in such a way that U is a monomorphism and not an automorphism (see [80, 108] for details). Changing the coordinates linearly, we obtain that $q(X) = p(Y) = y_1^2 + y_2^2 + y_3^2$ over $K[\sqrt{-1}]$. Extending U acting identically on $x_3, \ldots, x_n$, we obtain that over an algebraically closed field of characteristic zero the quadratic forms of maximal rank n are not test polynomials in the class of all monomorphisms of $K[x_1, \ldots, x_n]$ for $n \geq 3$.

Proposition 10.1.3. *Let K be a field of characteristic zero. Then the polynomial $x_1^2 + x_2^2$ is a test polynomial for automorphisms of $K[x_1, x_2]$ in the class of all endomorphisms without constant terms. It distinguishes the orthogonal linear transformations only.*

Proof. Let L be an extension of the base field K that contains $\sqrt{-1}$. If $p(X) = x_1^2 + x_2^2$ is a test polynomial for automorphisms in the class of all endomorphisms without constant terms over L, then $p(X)$ has the same property over K. Hence, without loss of generality, we may assume that $\sqrt{-1} \in K$. Let $F = (f_1, f_2)$ be such an endomorphism and let $p(F) = p(X)$. Then

$$p(F) = (f_1 + f_2\sqrt{-1})(f_1 - f_2\sqrt{-1}) = p(X) = (x_1 + x_2\sqrt{-1})(x_1 - x_2\sqrt{-1})$$

and we get

$$f_1 + f_2\sqrt{-1} = \alpha(x_1 \pm x_2\sqrt{-1}), \quad f_1 - f_2\sqrt{-1} = \alpha^{-1}(x_1 \mp x_2\sqrt{-1}), \quad 0 \neq \alpha \in K,$$

and F is a linear transformation of X. Since it fixes the quadratic form $p(X)$, it is orthogonal. ■

Proposition 10.1.4. *Every homogeneous polynomial of rank 2 with degree $d > 2$ is a test polynomial of $\mathbb{C}[x_1, x_2]$ for automorphisms of $\mathbb{C}[x_1, x_2]$ in the class of all endomorphisms without constant terms.*

Finally, we give a large class of test polynomials for $K[X]$.

Theorem 10.1.5.

(i) *Let K be any field, and let $k_1, \ldots, k_n$ be positive integers. Then the polynomial*

$$p(X) = X^k = x_1^{k_1} \ldots x_n^{k_n}$$

is a test polynomial for automorphisms in the class of all endomorphisms of $K[X] = K[x_1, \ldots, x_n]$ without constant terms. This test polynomial distinguishes the following automorphisms:

$$F = (\alpha_1 x_{\sigma(1)}, \ldots, \alpha_n x_{\sigma(n)}), \quad 0 \neq \alpha_1, \ldots, \alpha_n \in K,$$

where $\alpha_1^{k_1} \ldots \alpha_n^{k_n} = 1$, and σ is an element of the symmetric group S_n such that $k_{\sigma(1)} = k_1, \ldots, k_{\sigma(n)} = k_n$.

(ii) *The polynomial*

$$p(X) = (X^k)^s = (x_1^{k_1} \ldots x_n^{k_n})^s$$

with $k_i = n + i - 1$, $i = 1, \ldots, n$, and $s \geq 1$ is a test polynomial for automorphisms in the class of all endomorphisms of $K[X]$. The only automorphisms distinguished by these test polynomials are

$$F = (\alpha_1 x_1, \ldots, \alpha_n x_n), \quad (\alpha_1^{k_1} \ldots \alpha_n^{k_n})^s = 1, \quad \alpha_1, \ldots, \alpha_n \in K.$$

Proof.

(i) Let $F = (f_1, \ldots, f_n)$ be an endomorphism without constant terms. Then

$$p(F) = p(X), \quad f_1^{k_1} \ldots f_n^{k_n} = x_1^{k_1} \ldots x_n^{k_n}$$

gives immediately that $f_i = \alpha_i x_{\sigma(i)}$, $\sigma \in S_n$. The end of the statement follows by comparison of the degrees of the variables in $p(X)$.

(ii) Let $F = (f_1, \ldots, f_n)$ and $(f_1^{k_1} \ldots f_n^{k_n})^s = (x_1^{k_1} \ldots x_n^{k_n})^s$. Then all polynomials f_i are monomials. Let

$$f_i = \beta_i \prod_{j=1}^{n} x_j^{a_{ij}}, \quad 0 \neq \beta \in K, \quad \prod_{i=1}^{n} x_i^{k_i} = \prod_{i=1}^{n} \prod_{j=1}^{n} x_j^{a_{ij}},$$

and we obtain for the degree of x_i that

$$a_{i1} n + a_{i2}(n+1) + \cdots + a_{in}(2n-1) = n + i - 1.$$

Since all a_{ij} are nonnegative integers and the sum of any two $n + q - 1$ and $n + r - 1$ is bigger than $2n - 1$, we obtain the only possibility, $a_{ii} = 1$, $a_{ij} = 0$, $i \neq j$, and this completes the proof. ∎

Remark 10.1.6. The statement (i) of the previous theorem is not true in the class of all endomorphisms. For example, the polynomial $p(X) = x_1 \dots x_n$ is fixed by the endomorphism $F = (x_1 \dots x_n, 1, \dots, 1)$, which is not an automorphism for $n > 1$.

Remark 10.1.7. Using the idea of the proof of Theorem 10.1.5 (ii), we can also construct test polynomials for nonlinear triangular automorphisms. For example, let $n = 2$,

$$p(X) = x_2^2(x_1 + a^2(1 - a^8)^{-1}x_2^2)^3, \quad a \in K, \quad a \neq 0, \quad a^8 \neq 1.$$

Easy calculations show that $p(X)$ is fixed by the automorphism

$$F = (a^{-2}x_1 + x_2^2, a^3x_2).$$

On the other hand, arguments similar to those in the proof of Theorem 10.1.5 (ii) show that $p(X)$ is a test polynomial for automorphisms in the class of all endomorphisms. The automorphism F is conjugated in $\mathrm{Aut}\, K[x_1, x_2]$ to a linear automorphism. If we introduce a new system of generators

$$Y = (y_1, y_2) = (x_1 + a^2(1 - a^8)^{-1}x_2^2, x_2),$$

we see that $F(Y) = (a^{-2}y_1, a^3y_2)$. On the other hand, by [108], any triangular automorphism $F = (x_1 + h_1, \dots, x_n + f_n)$, $h_i \in K[x_{i+1}, \dots, x_n]$ cannot be recognized by a test polynomial.

10.2 Test Elements in Free Associative Algebras

We start with some background on the structure and combinatorial properties of the free associative algebra $K\langle X\rangle = K\langle x_1, \dots, x_n\rangle$ over an arbitrary field K.

Proposition 10.2.1 ([80]).

(i) *The algebra $K\langle X\rangle$ is an FIR (a free ideal ring); i.e., any left (right) ideal I is a free left (right) $K\langle X\rangle$-module. If I is generated by a system of homogeneous elements, then I has a system of homogeneous free generators as a $K\langle X\rangle$-module.*

(ii) *If $0 \neq y_i, z_i \in K\langle X\rangle$, $i = 1, \dots, k$, $\deg(y_{i-1}) \leq \deg(y_i)$, $i = 2, \dots, k$, and $\sum_{i=1}^{k} y_i z_i = 0$, then one of the elements y_i belongs to the right ideal generated by $y_1, \dots, y_{i-1}$.*

Corollary 10.2.2.

(i) *If u_i, v_i, $i = 1, 2$, are nonzero elements of $K\langle X\rangle$ and $\deg(u_1) \geq \deg(v_1)$, then the equality $u_1u_2 = v_1v_2$ implies that $u_1 = v_1w$, $v_2 = wu_2$ for some $w \in K\langle X\rangle$.*

(ii) *If* $\operatorname{char} K = 0$ *and* $uv + vu = 0$ *in* $K\langle X\rangle$, *then* $u = 0$ *or* $v = 0$.

Proof. The statement of (i) follows directly from Proposition 10.2.1 (ii).

(ii) We use induction on $\deg(u) + \deg(v)$, the base of the induction $\deg(v) = 0$ being trivial. Let $u, v \neq 0$ and $\deg(u) \geq \deg(v) \geq 1$. Since $uv = v(-u)$, by (i), $u = vw$ for some $w \in K\langle X\rangle$ and $(vw)v + v(vw) = 0$. Since $K\langle X\rangle$ has no zero divisors, we obtain that $wv + vw = 0$. Now $\deg(w) < \deg(u)$, and this completes the proof. ■

Theorem 10.2.3. *Let* K *be a field of characteristic* 0. *Then the element* $p(X) = x_1^2 + x_2^2$ *is a test element for automorphisms of the free algebra* $K\langle x_1, x_2\rangle$ *in the class of all endomorphisms without constant terms.*

Proof. As in the proof of Proposition 10.1.3, we assume that $\sqrt{-1} \in K$. Let $F = (f_1, f_2)$ be an endomorphism without constant terms and such that $p(F) = p(X)$. Let

$$f_1 = g_1 + g_2 + \cdots + g_k, \quad f_2 = h_1 + h_2 + \cdots + h_k,$$

where g_i and h_i are the homogeneous components of degree i of f_1 and f_2, respectively. If $h_k \neq 0$ and $k > 1$, by comparing the homogeneous components of degree $2k$ of $p(F)$ and $p(X)$, we obtain that $g_k^2 + h_k^2 = 0$; i.e., $g_k = h_k\sqrt{-1}$. Now we apply inductive argument. We assume that for some $i \geq 1$ we have established $g_j = h_j\sqrt{-1}$, $j = i+1, \ldots, k$. The comparison of the homogeneous components of degree $k + i$ gives

$$\sum_{s=i}^{k} (g_s g_{i+k-s} + h_s h_{i+k-s}) = 0,$$

$$(h_i + g_i\sqrt{-1})h_k + h_k(h_i + g_i\sqrt{-1}) = 0.$$

By Corollary 10.2.2 (ii), $g_i = h_i\sqrt{-1}$. In this way we establish that $g_1 = h_1\sqrt{-1}$. The homogeneous components of degree 2 of $p(F)$ and $p(X)$ satisfy the equality $g_1^2 + h_1^2 = x_1^2 + x_2^2$, which contradicts $g_1 = h_1\sqrt{-1}$. Therefore the map F is linear. Since it leaves invariant the quadratic form $x_1^2 + x_2^2$, it is invertible, and this means that F is an automorphism. ■

Now we construct a family of multilinear test polynomials recognizing automorphisms in the class of endomorphisms without constant terms.

Theorem 10.2.4. *Let* K *be a field of characteristic* 0 *and let*

$$p(X) = \sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} \ldots x_{\sigma(n)} \in K\langle X\rangle = K\langle x_1, \ldots, x_n\rangle,$$

where $\alpha_\sigma \in K$ *and* S_n *is the symmetric group of degree* n. *If* $\sum_{\sigma \in S_n} \alpha_\sigma \neq 0$, *then* $p(X)$ *is a test element that recognizes automorphisms in the class of all endomorphisms without constant terms. This test element distinguishes linear automorphisms only.*

Proof. Let $F = (f_1, \dots, f_n)$ be an endomorphism without constant terms such that $p(F) = p(X)$. First we assume that F is not linear. Let g_i be the homogeneous component of f_i of maximal degree. Since the element $p(X)$ is multilinear, the homogeneous component of maximal possible degree of $p(F) = p(f_1, \dots, f_n)$ is equal to $p(G) = p(g_1, \dots, g_n)$. Since F is not linear, $\deg(g_i) > 1$ for some i, and we obtain

$$p(G) = p(g_1, \dots, g_n) = \sum_{\sigma \in S_n} \alpha_\sigma g_{\sigma(1)} \dots g_{\sigma(n)} = 0.$$

Hence, for any $\tau \in S_n$,

$$p(\tau(G)) = p(g_{\tau(1)}, \dots, g_{\tau(n)}) = \sum_{\sigma \in S_n} \alpha_\sigma g_{\sigma\tau(1)} \dots g_{\sigma\tau(n)} = 0.$$

We make a summation of these equalities allowing τ to run through S_n and, since $S_n\tau = S_n$, we obtain

$$q(G) = \Big(\sum_{\rho \in S_n} \alpha_\rho \Big) \Big(\sum_{\sigma \in S_n} g_{\sigma(1)} \dots g_{\sigma(n)} \Big) = 0.$$

Therefore, we may assume that in the equality $p(G) = 0$ all coefficients α_σ are equal to 1; i.e.,

$$p(X) = \sum_{\sigma \in S_n} x_{\sigma(1)} \dots x_{\sigma(n)}.$$

Let h_i be the leading term of g_i with respect to the lexicographical order. Then the leading term of every product $g_{\sigma(1)} \dots x_{\sigma(n)}$ in $p(G)$ is $h_{\sigma(1)} \dots h_{\sigma(n)}$ and the leading term of $p(G)$ is a sum of some $h_{\sigma(1)} \dots h_{\sigma(n)}$. Since the base field is of characteristic 0, we obtain that the leading term of $p(G)$ is different from 0, which is a contradiction. In this way we establish that all polynomials f_i are linear. Now the map F induces a map $\bar{F} = (\bar{f}_1, \dots, \bar{f}_n)$ of the polynomial algebra $K[\bar{X}]$ and

$$\bar{p}(\bar{X}) = \bar{p}(\bar{F}) = n!\bar{f}_1 \dots \bar{f}_n.$$

By using Theorem 10.1.5, we see that the polynomials in commuting variables $\bar{f}_i$ are linearly independent. Since f_i are linear, this implies that f_i are also linearly independent; i.e., F is a linear automorphism of $K\langle X \rangle$. This completes the proof of the theorem. ∎

Remark 10.2.5. As in the commutative case, the statement of Theorem 10.2.4 does not hold if we consider the class of all endomorphisms of the free algebra.

Corollary 10.2.6. *Let K be a field of characteristic* 0, *and let*

$$p(X) = \sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} \dots x_{\sigma(n)} \in K\langle X \rangle = K\langle x_1, \dots, x_n \rangle,$$

where $\alpha_\sigma \in K$, S_n *is the symmetric group of degree* n, *and* $\sum_{\sigma \in S_n} \alpha_\sigma \neq 0$. *For any fixed* $s \geq 1$, *the element*

$$q(X) = p(x_1^{sn}, x_2^{s(n+1)}, \ldots, x_n^{s(2n-1)})$$

is a test element that recognizes automorphisms in the class of all endomorphisms.

Proof. Let F be an endomorphism of $K\langle X\rangle$ such that $q(F) = q(X)$ and let $G = (g_1, \ldots, g_n)$, where $g_i = f_i^{s(n+i-1)}$. Let h_i be the homogeneous component of maximum degree of g_i. If F is not affine, as in the proof of Theorem 10.2.4, we obtain $p(h_1, \ldots, h_n) = 0$, which is impossible. Hence F is affine. Now we consider the endomorphism $\bar{F}$ of $K[\bar{X}]$ induced by F. Clearly,

$$\begin{aligned}
\bar{q}(\bar{X}) = \bar{q}(\bar{F}) = \bar{p}(\bar{G}) &= \Big(\sum_{\sigma \in S_n} \alpha_\sigma\Big) \bar{g}_1 \ldots \bar{g}_n \\
&= \Big(\sum_{\sigma \in S_n} \alpha_\sigma\Big) \bar{f}_1^{sn} \bar{f}_2^{s(n+1)} \ldots \bar{f}_n^{s(2n-1)} \\
&= \Big(\sum_{\sigma \in S_n} \alpha_\sigma\Big) \bar{x}_1^{sn} \bar{x}_2^{s(n+1)} \ldots \bar{x}_n^{s(2n-1)}.
\end{aligned}$$

Applying Theorem 10.1.5 again, we obtain that $\bar{F}$ is a linear automorphism of $K[\bar{X}]$, and the same holds for F in $K\langle X\rangle$. ■

Up to conjugation, most of the examples of test polynomials in the commutative case recognize linear automorphisms only. Now we construct a family of automorphisms of $K\langle X\rangle$ that recognize larger classes of automorphisms. The construction is based on the result of Dicks [93] that the commutator $[x_1, x_2]$ is a test polynomial that, up to a multiplicative constant, distinguishes automorphisms of $K\langle x_1, x_2\rangle$ in the class of all endomorphisms.

Lemma 10.2.7. *Let* $n > 2$ *and let every monomial of* $h_1, h_2 \in K\langle X\rangle$ *depend essentially on some of the variables* $x_3, \ldots, x_n$. *Then the equality*

$$[x_1 + h_1, x_2 + h_2] = [x_1, x_2]$$

implies $h_1 = h_2 = 0$.

Proof. Without loss of generality, we may assume that $h_1 \neq 0$. Let $W \subset K\langle X\rangle$ be the vector space spanned on all monomials that depend on some $x_3, \ldots, x_n$. Every monomial from W can be written in the form

$$w = w_1(x_1, x_2) x_{i_1} \ldots x_{i_k} w_2(x_1, x_2), \quad k \geq 1,$$

where w_1 and w_2 depend on x_1 and x_2 only and both the indices i_1 and i_k are different from 1 and 2. Obviously, W is a free $K\langle x_1, x_2\rangle$-bimodule with

basis consisting of all monomials

$$x_{i_1} \dots x_{i_k}, \quad k \geq 1, \quad i_1, i_k \neq 1, 2.$$

Let p be the minimal degree of the nonzero homogeneous components of h_1 and h_2, and let u_1 and u_2 be the homogeneous components of degree p of h_1 and h_2, respectively. Clearly,

$$[x_1, u_2] + [u_1, x_2] = x_1 u_2 - x_2 u_1 - u_2 x_1 + u_1 x_2 = 0.$$

We express u_1 and u_2 in the form

$$u_1 = \sum s_{1i}(x_1, x_2) x_{i_1} \dots x_{i_k} s_{2i}(x_1, x_2),$$
$$u_2 = \sum t_{1i}(x_1, x_2) x_{i_1} \dots x_{i_k} t_{2i}(x_1, x_2),$$

where the summation runs over all $i_1, \dots, i_k$ with $i_1, i_k \neq 1, 2$. Therefore,

$$[x_1, u_2] + [u_1, x_2] = \sum (x_1 s_{1i} x_{i_1} \dots x_{i_k} s_{2i} - x_2 t_{1i} x_{i_1} \dots x_{i_k} t_{2i}$$
$$- s_{1i} x_{i_1} \dots x_{i_k} s_{2i} x_1 + t_{1i} x_{i_1} \dots x_{i_k} t_{2i} x_2) = 0.$$

Since W is a free $K\langle x_1, x_2\rangle$-bimodule, for any fixed $(i_1, \dots, i_k)$ we obtain the following equality in $K\langle x_1, x_2\rangle \otimes_K K\langle x_1, x_2\rangle$:

$$x_1 s_{1i} \otimes s_{2i} - x_2 t_{1i} \otimes t_{2i} - s_{1i} \otimes s_{2i} x_1 + t_{1i} \otimes t_{2i} x_2 = 0.$$

By comparing the homogeneous components of minimum degree of s_{2i} and t_{2i}, we obtain that they are 0, which is a contradiction. This completes the proof of the lemma. ■

Theorem 10.2.8. *Let $i_1, \dots, i_r, j_1, \dots, j_r$ be a set of indices such that $i_k \neq j_k$, $k = 1, \dots, r$, and*

$$\{i_k, j_k \mid k = 1, \dots, r\} = \{1, \dots, n\}.$$

Then the polynomial

$$p(X) = [x_{i_1}, x_{j_1}] \dots [x_{i_r}, x_{j_r}]$$

is a test polynomial recognizing automorphisms in the class of all endomorphisms of $K\langle X\rangle$.

Proof. Let $F = (f_1, \dots, f_n)$ be an endomorphism of $K\langle X\rangle$ such that $p(F) = p(X)$. Since the commutators $[f_{i_k}, f_{j_k}]$ have no constant and linear terms and $\deg(p(X)) = 2r$, we obtain

$$[f_{i_k}, f_{j_k}] = \alpha_k [x_{i_k}, x_{j_k}], \quad 0 \neq \alpha_k \in K.$$

For example, let $[f_1, f_2] = \alpha[x_1, x_2]$. We write f_1 and f_2 in the form

$$f_1 = g_1(x_1, x_2) + h_1, \quad f_2 = g_2(x_1, x_2) + h_2,$$

where each monomial of h_1, h_2 depends on some of the variables $x_3, \dots, x_n$. Therefore,

$$[g_1(x_1, x_2), g_2(x_1, x_2)] = \alpha[x_1, x_2]$$

and, by the result of Dicks [93], (g_1, g_2) is an automorphism of $K\langle x_1, x_2\rangle$. We extend it to an automorphism $G = (g_1, g_2, x_3, \dots, x_n)$ of $K\langle X\rangle$. Let $G^{-1} = (u_1, u_2, x_3, \dots, x_n)$ be the inverse of G. Clearly, $[u_1, u_2] = \alpha^{-1}[x_1, x_2]$ and the composition of automorphisms $V = F \circ G^{-1}$ has the property $[v_1, v_2] = [x_1, x_2]$. On the other hand, it is easy to see that

$$v_1 = x_1 + w_1, v_2 = x_2 + w_2,$$

where each monomial of w_1, w_2 depends on some $x_3, \dots, x_n$. By Lemma 10.2.7, this implies that $w_1 = w_2 = 0$; i.e., $f_1 = f_1(x_1, x_2)$, $f_2 = f_2(x_1, x_2)$, and (f_1, f_2) is an automorphism of $K\langle x_1, x_2\rangle$. In this way, we obtain that for each pair of indices i_k, j_k, the pair $F_k = (f_{i_k}, f_{j_k})$ belongs to $(K\langle x_{i_k}, x_{j_k}\rangle)^2$ and induces an automorphism of $K\langle x_{i_k}, x_{j_k}\rangle$.

Now, if any index i appears exactly once in the indices $i_1, \dots, i_r$, $j_1, \dots, j_r$, we obtain that F is decomposed as a product of automorphisms G_k such that each G_k fixes all x_s different from x_{i_k} and x_{j_k} and $f_{i_k}, f_{j_k} \in K\langle x_{i_k}, x_{j_k}\rangle$. Therefore, F is an automorphism. If, for example, the index 1 appears twice, say as i_1 and i_2, then $f_1 \in K\langle x_1, x_{j_1}\rangle \cap K\langle x_1, x_{j_2}\rangle$ and $f_1 = f_1(x_1)$. Since (f_1, f_{j_1}) is an automorphism of $K\langle x_1, x_{j_1}\rangle$, we obtain that $f_1 = \xi + \eta x_1$, $\xi, \eta \in K$, $\eta \neq 0$, and f_i is a linear polynomial in x_1. Now $p(X)$ is presented as a product of three kinds of commutators:

(i) $[x_i, x_j]$, where the variables x_i and x_j appear in other commutators as well;

(ii) $[x_i, x_k]$, where x_i appears in other commutators, whereas x_k does not;

(iii) $[x_l, x_m]$, where neither x_l nor x_m appear in other commutators.

As a result of our observations, we obtain that

$$f_i = \xi_i + \eta_i x_i, \quad f_j = \xi_j + \eta_j x_j, \quad \xi_i, \xi_j \in K, \quad 0 \neq \eta_i, \eta_j \in K;$$
$$f_k = \eta_k x_k + g_k(x_i), \quad 0 \neq \eta_k \in K, \quad g_k \in K\langle x_i\rangle,$$
$$(f_l, f_m) = (f_l(x_l, x_m), f_m(x_l, x_m)) \in \operatorname{Aut} K\langle x_l, x_m\rangle.$$

Again, F is a composition of automorphisms that fix all but one or two of the variables, and this implies that F itself is an automorphism. ■

The following corollary is an analog of a result of Zieschang [417] in the case of free groups.

Corollary 10.2.9. *The element*

$$p(X) = [x_1, x_2] \dots [x_{2n-1}, x_{2n}]$$

is a test element in the class of all endomorphisms of $K\langle x_1, \dots, x_{2n}\rangle$.

10.3 Open Problems

Problem 10.3.1. Is the element

$$p(X) = x_1^2 + \cdots + x_n^2, \quad X = (x_1, \ldots, x_n), \quad n > 2,$$

a test element for automorphisms in the class of endomorphisms of $K\langle X\rangle$ without constant terms over any field of characteristic 0? By Example 10.1.2, this is not true for $K[X]$ when K is algebraically closed.

Problem 10.3.2. Let $X = \{x_1, \ldots, x_{2n}\}$,

$$u = [x_1, x_2] + [x_3, x_4] + \cdots + [x_{2n-1}, x_{2n}].$$

Is u a test element of the free associative algebra $K\langle X\rangle$?

Problem 10.3.3. Let F be an automorphism of $K[X]$, $\operatorname{char} K = 0$, and let $p(X)$ be a test polynomial for F. Is F conjugate to a diagonalizable linear automorphism?

Problem 10.3.4. Let $F = (x_1 + h_1, \ldots, x_n + h_n)$ be a triangular automorphism of $K\langle X\rangle$, where the elements h_i do not depend on $x_1, \ldots, x_i$, and let F be nonaffine; i.e., some of the elements h_i are of degree ≥ 2. Is there a test element recognizing F in the class of all endomorphisms with or without constant terms? By [108], in the commutative case, F has no test polynomials.

Problem 10.3.5. Describe linear automorphisms that possess test polynomials. Is it true that a diagonal automorphism

$$G = (\xi_1 x_1, \ldots, \xi_n x_n), \quad 0 \neq \xi_i \in K, \quad i = 1, \ldots, n,$$

has a test polynomial if and only if there exist positive integers $k_1, \ldots, k_n$ such that

$$\xi_1^{k_1} \ldots \xi_n^{k_n} = 1?$$

Conjecture 10.3.6. For $n > 2$, the standard polynomial

$$s_n(X) = s_n(x_1, \ldots, x_n) = \sum_{\sigma S_n} (\operatorname{sign} \sigma) x_{\sigma(1)} \ldots x_{\sigma(n)}$$

is a test element for $K\langle X\rangle$, $X = \{x_1, \ldots, x_n\}$. It has the property that for an endomorphism F of $K\langle X\rangle$,

$$s_n(F) = \alpha s_n(X), \quad 0 \neq \alpha \in K$$

if and only if F is linear and invertible for n odd and F is affine and invertible for n even, $n > 2$.

Conjecture 10.3.7. Any nontrivial multilinear polynomial of degree n is a test element for automorphisms of $K\langle X\rangle$, $X = \{x_1, \ldots, x_n\}$ in the class of all endomorphisms without constant terms.

Conjecture 10.3.8. Any nontrivial multihomogeneous polynomial $p(X)$ that depends essentially on all variables X is a test polynomial for automorphisms of $K\langle X\rangle$, $X = \{x_1, \dots, x_n\}$ in the class of all endomorphisms without constant terms. If $\deg_{x_i}(p) = n + i - 1$, $i = 1, \dots, n$, then $p(X)$ is a test element in the class of all endomorphisms.

Problem 10.3.9. Is it true that for any automorphism F of $K\langle X\rangle$ (or for any tame automorphism) there exists a test element $p(X)$ (in some class of endomorphisms) such that

$$p(F) = \alpha p(X), \quad 0 \neq \alpha \in K?$$

For example, is the element

$$p(x_1, x_2, x_3) = [x_1, f_1(x_2, x_3)][x_2, x_3], \quad f(0,0) \neq 0$$

a test element recognizing $F = (x_1 + f_1(x_2, x_3), x_2, x_3)$?

A polynomial $P \in \mathbb{C}[X]$ of degree d is called a *general polynomial* in $\mathbb{C}[X]$ if the coefficients $a_{i_1 \dots i_n}$ of all monomials $x_1^{i_1} \dots x_n^{i_n}$ with $0 \leq i_1 + \dots + i_n \leq d$ in

$$P = \sum_{0 \leq i_1 + \dots + i_n \leq d} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$$

are nonzero and algebraically independent over $\mathbb{Q}$.

Conjecture 10.3.10. Let $P \in \mathbb{C}[x_1, \dots, x_n]$ be a general polynomial of degree $d \geq n > 2$. Then P is a test polynomial recognizing only the identical automorphism.

Part III

Free Nielsen–Schreier Algebras

Introduction to Part III

In this part of the book, we study free algebras of Schreier varieties of algebras.

Let K be a field. A variety $\mathfrak{M}$ of algebras over K is defined as a class of algebras closed under taking subalgebras, homomorphic images, and direct products. Let X be a set. An algebra $F_{\mathfrak{M}}(X)$ in $\mathfrak{M}$ is a free algebra with the set X of free generators if $F_{\mathfrak{M}}(X)$ is generated by X, and if f is an arbitrary map from X to any algebra A of $\mathfrak{M}$, then f can be extended to a homomorphism $F_{\mathfrak{M}}(X) \to A$ (it is clear that such extension is unique). The algebra $F_{\mathfrak{M}}(X)$ is determined by X and $\mathfrak{M}$ uniquely up to an isomorphism. The cardinality of X is called the rank of $F_{\mathfrak{M}}(X)$. For any nontrivial variety $\mathfrak{M}$ and a set X, there exists the free algebra $F_{\mathfrak{M}}(X)$. If $A \in \mathfrak{M}$, then there exists a set X such that A is a homomorphic image of $F_{\mathfrak{M}}(X)$. In particular, A is isomorphic to a factor algebra of $F_{\mathfrak{M}}(X)$.

Let X be a finite set, $X = \{x_1, \ldots, x_n\}$. A pair (u, v) of elements of $F_{\mathfrak{M}}(X)$ is called an identity in an algebra A of $\mathfrak{M}$ if $u(a_1, \ldots, a_n) = v(a_1, \ldots, a_n)$ for all elements $a_1, \ldots, a_n$ of A. The following result is due to G. Birkhoff. Let $\mathfrak{M}$ be a variety of algebras. A subclass $\mathfrak{N}$ in $\mathfrak{M}$ is a (sub)variety if and only if there exists a set of identities (u_i, v_i), $i \in I$, such that $\mathfrak{N}$ consists of all algebras of $\mathfrak{M}$ satisfying these identities. Here u_i, v_i $(i \in I)$ are elements of $F_{\mathfrak{M}}$ with a countable set X of free generators. A variety of algebras is called homogeneous if it is defined by a set of homogeneous identities. A variety of algebras is said to be Schreier if any subalgebra of a free algebra of this variety is free in the same variety of algebras.

Chapter 11 considers basic properties of free algebras of homogeneous Schreier varieties of algebras. In Section 11.1, we describe the main types of Schreier varieties and introduce universal multiplicative enveloping algebras of free algebras. In Section 11.2, we expose the weak algorithm for free associative algebras and discuss Schreier's techniques for free algebras: ranks of left ideals of free associative algebras and Schreier-type formulas for ranks of subalgebras of free algebras.

Using free differential calculus, we introduce partial derivatives of elements of free algebras in Section 11.3. We show that free algebras of the main types of Schreier varieties have the property of differential separability for subalgebras. At the same time, free Lie superalgebras are residually finite. Theorems 11.3.6–11.3.8 give some necessary and sufficient conditions for a homogeneous variety of algebras to be Schreier. Theorem 11.3.11 gives an effective algorithm to find ranks of subalgebras of free algebras. In Section 11.4, we consider equivalence and stable equivalence of elements under the action of the automorphism group. Section 11.5 shows that an injective endomorphism of maximal rank does not change the rank of a system of elements of maximal rank.

In Chapter 12, we consider automorphic orbits and combinatorial properties of primitive elements in free algebras of the main types of Schreier varieties of algebras. A system of elements of a free algebra F is primitive if it is a subset of some set of free generators of F. The rank of a system of elements of a free algebra F is the minimal number of generators from X on which automorphic images of these elements can depend.

Let A be a finitely generated free algebra of the variety $\mathfrak{M}_0$ (the variety of all algebras), $\mathfrak{M}_1$ (the variety of all commutative algebras, $\operatorname{char} K \neq 2$), or $\mathfrak{M}_2$ (the variety of all anticommutative algebras).

In Sections 12.1 and 12.2, we consider basic properties of partial derivatives of elements of A. Section 12.3 is devoted to elimination of variables.

In Section 12.4, we obtain the rank theorems. Theorems 12.4.7 and 12.4.8 show that the rank of a system of elements is equal to the rank of the free module generated by the elements whose components are partial derivatives of elements of this system. Theorems 12.4.9 and 12.4.10 are the rank theorems for free Lie algebras and superalgebras.

In Section 12.5, we study primitive systems of elements and actions of endomorphisms on automorphic orbits of elements. Theorem 12.5.1 gives a matrix characterization of primitive systems of elements: a system of elements of A is primitive if and only if the matrix of partial derivatives of elements of the system is left invertible over $U(A)$. Based on Theorems 12.4.7–12.5.1, we obtain in Theorem 12.5.2 algorithms to find the rank of a system of elements and to decide whether this system is primitive or not. Theorems 12.5.3–12.5.8 give matrix characterizations of primitive systems of elements in free Lie algebras and superalgebras. Using the Freiheitssatz, we obtain another characterization of primitive elements

in Theorem 12.5.15: an element a of A is primitive if and only if the factor algebra of A by the ideal generated by a is a free algebra in the same variety of algebras.

In Section 12.6, we consider actions of endomorphisms on primitive elements: endomorphisms of A preserving primitivity of elements are automorphisms (this statement is also true for free Lie algebras and superalgebras). Using this result, we obtain a more general statement in Section 13.3 of Chapter 13. Theorem 13.3.3 says that if an endomorphism of A preserves the automorphic orbit of a nonzero element, then it is an automorphism of A. In Theorems 12.6.6–12.6.8 and Problems 12.6.9 and 12.6.10, we consider images of nonzero linear combinations of free generators.

In Chapter 13, we consider fixed points of endomorphisms and automorphisms of free algebras and generalized primitive elements. Let K be a field, $\operatorname{char} K \neq 2$, and let X be a finite set, $X = \{x_1, \ldots, x_n\}$, $F = F(X)$ the free K-algebra without the unity element on the set X of free generators of one of the following varieties of algebras over a field K: the variety of all algebras, the variety of Lie algebras, varieties of color Lie superalgebras, the variety of Lie p-algebras, varieties of color Lie p-superalgebras, and varieties of commutative and anticommutative algebras.

A subalgebra H of F is said to be a retract if there is a homomorphism $\rho\colon F \to H$ such that ρ is the identity mapping on H (ρ is the retraction homomorphism). Obviously, a subalgebra H of F is a retract if and only if there exists an ideal I of F such that $F = H \oplus I$.

In Section 13.1, we consider test elements of the algebra $F = F(X)$: we prove that test elements for monomorphisms of the algebra F are the elements of the maximal rank (Theorem 13.1.1); test elements for endomorphisms of F are elements that do not belong to any proper retract of F (Theorem 13.1.4). Section 13.2 characterizes retracts of the algebra F (Theorem 13.2.1). In Section 13.3, we prove that if an endomorphism φ of the algebra F preserves the automorphic orbit of a nonzero element of F, then actually φ is an automorphism (Theorems 13.3.1–13.3.3).

After that, we study generalized primitive elements of free algebras and their automorphic orbits. An almost primitive element (APE) of a free algebra F is an element that is not primitive in F but is primitive in any proper subalgebra of F containing it. Section 13.4 deals with almost primitive and test elements of free algebras with the Nielsen–Schreier property. We show that almost primitive elements are elements of maximal rank. If the free algebra F is a free product of its subalgebras A and B, and elements a and b are homogeneous almost primitive elements in algebras A and B, respectively, then the element $a + b$ is an almost primitive element in F. This result gives us a possibility to construct in Theorem 13.4.7 a series of almost primitive elements. We discuss also a connection between properties of elements to be almost primitive and to be test elements.

By Δ we denote the left ideal of the free associative algebra $K\langle X\rangle$ generated by the set X. Following [356], we say that an element u of $L(X)$ is a Δ-primitive element if the elements $\frac{\partial}{\partial x_1}u, \ldots, \frac{\partial}{\partial x_n}u$ generate Δ as the left ideal of $K\langle X\rangle$.

In Section 13.5, we prove Theorem 13.5.1: If the rank n of the free Lie algebra L is even, $n = 2m$, then any Δ-primitive element of L is an automorphic image of $[x_1, x_2] + \cdots + [x_{2m-1}, x_{2m}]$, there are no Δ-primitive elements of L if n is odd, and the automorphism group of the algebra L acts transitively on the set of all Δ-primitive elements.

In Section 13.6, we consider generic elements of free Lie algebras. Let $\mathfrak{U}$ be a variety of Lie algebras over a field K defined by the set of identities $\mathfrak{V}$, $L = L(X)$ the free Lie algebra with the set X of free generators, and let $\mathfrak{V}(L)$ be the verbal ideal of L defined by $\mathfrak{V}$. An element f of L is said to be $\mathfrak{U}$-generic if $f \in \mathfrak{V}(L)$ but $f \notin \mathfrak{V}(H)$ for every proper subalgebra H of L. Let $\mathfrak{A}$ be the variety of abelian Lie algebras. An element u of the free Lie algebra L is $\mathfrak{A}$-generic if $u \in [L, L]$, and if $u \in [H, H]$ for some subalgebra H of L, then $H = L$. Propositions 13.6.1 and 13.6.3 give new examples of almost primitive elements of free Lie algebras. In Proposition 13.6.4 and Theorem 13.6.5, we construct series of examples of $\mathfrak{A}$-generic elements of free Lie algebras. Theorem 13.6.7 gives an example of an $\mathfrak{A}$-generic element of the free Lie algebra $L(x, y)$ that is not an APE of this algebra. In Theorem 13.6.8, we show that the element $u = [x_1, \ldots, x_n]$ is an $\mathfrak{N}_n$-generic element of the free Lie algebra $L(X)$, where $\mathfrak{N}_n$ is the variety of nilpotent Lie algebras of degree not less than n.

Chapter 14 considers free Leibniz algebras and their automorphisms. Let K be a field and L a K-algebra with the bracket multiplication $[\,,\,]$. Then L is a Leibniz algebra if

$$[x, [y, z]] = [[x, y], z] - [[x, z], y]$$

for all $x, y, z \in L$.

The variety of Leibniz algebras is not a Schreier variety of algebras. Nevertheless, many combinatorial properties of this variety are similar to the properties of Schreier varieties of algebras.

In Section 14.2, we prove that the variety of all Leibniz algebras has the property of differential separability for subalgebras, Theorem 14.2.1. Theorem 14.2.2 shows that the Jacobian conjecture has a positive solution for free Leibniz algebras.

In Section 14.3, we study finitely generated subalgebras of the free Leibniz algebra. An algebra R is called residually finite if for any element $a \in R$ and for any finitely generated subalgebra B such that $a \notin B$ there exist a finite-dimensional algebra H and a homomorphism $\varphi\colon R \to H$ such that $\varphi(a) \notin \varphi(B)$. Theorem 14.3.8 shows that free Leibniz algebras are residually finite. It follows that the occurrence problem for free Leibniz algebras is algorithmically decidable.

In order to clarify differences between the variety of Leibniz algebras and the Schreier variety of algebras, we consider automorphisms of free Leibniz algebras in Section 14.4. Automorphisms of finitely generated free algebras of Schreier varieties of algebras are tame; that is, they are compositions of elementary automorphisms (see Section 11.1 of Chapter 11). In Section 14.4.1, Theorem 14.4.5 gives a characterization of tame automorphisms. Section 14.4.2 collects corollaries of the main result. Theorem 14.4.7 shows that there is an algorithm to recognize tame automorphisms. Theorem 14.4.8 gives an example of a wild automorphism.

11
Schreier Varieties of Algebras

In this chapter, we consider the main properties of free algebras of Schreier varieties of algebras. A variety of algebras is said to be Schreier if any subalgebra of a free algebra of this variety is free in the same variety of algebras. In Section 11.1, we describe the main types of Schreier varieties and introduce universal multiplicative enveloping algebras of free algebras. Theorem 11.1.1 gives the main properties of the free algebras of these varieties. In Section 11.2, we expose the weak algorithm for free associative algebras and discuss Schreier's techniques for free algebras: ranks of left ideals of free associative algebras and Schreier-type formulas for ranks of subalgebras of free algebras.

Using free differential calculus, we introduce partial derivatives of elements of free algebras in Section 11.3. Theorem 11.3.1 shows that free algebras of the main types of Schreier varieties have the property of differential separability for subalgebras. Using the Poincaré–Birkhoff–Witt theorems, we prove in Theorem 11.3.4 that Lie superalgebras are differentially separable. Theorem 11.3.5 shows that free Lie superalgebras are residually finite. Theorems 11.3.6–11.3.8 give some necessary and sufficient conditions for a homogeneous variety of algebras to be Schreier. Theorem 11.3.11 gives an effective algorithm to find ranks of subalgebras of free algebras. In Section 11.4, we consider equivalence and stable equivalence of elements under the action of the automorphism group (Theorems 11.4.4 and 11.4.5).

Theorems 11.5.3 and 11.5.4 of Section 11.5 show that an injective endomorphism of maximal rank does not change the rank of a system of elements of maximal rank.

11.1 Main Types of Nielsen–Schreier Algebras

Let K be a field. A variety $\mathfrak{M}$ of algebras over K is a class of algebras closed under taking subalgebras, homomorphic images, and direct products. Let X be a set. An algebra $F_{\mathfrak{M}}(X)$ in $\mathfrak{M}$ is called the free algebra with the set X of free generators if $F_{\mathfrak{M}}(X)$ is generated by X, and if f is an arbitrary map from X to any algebra A of $\mathfrak{M}$, then f can be extended to a homomorphism $F_{\mathfrak{M}}(X) \to A$ (it is clear that such extension is unique). The algebra $F_{\mathfrak{M}}(X)$ is determined by X and $\mathfrak{M}$ uniquely up to an isomorphism. The cardinality of X is called the rank of $F_{\mathfrak{M}}(X)$. For any nontrivial variety $\mathfrak{M}$ and a set X there exists the free algebra $F_{\mathfrak{M}}(X)$. If $A \in \mathfrak{M}$, then there exists a set X such that A is a homomorphic image of $F_{\mathfrak{M}}(X)$. In particular, A is isomorphic to a factor algebra of $F_{\mathfrak{M}}(X)$.

Let X be a finite set, $X = \{x_1, \ldots, x_n\}$. A pair (u, v) of elements of $F_{\mathfrak{M}}(X)$ is an identity in an algebra A of $\mathfrak{M}$ if $u(a_1, \ldots, a_n) = v(a_1, \ldots, a_n)$ for all elements $a_1, \ldots, a_n$ of A. The following result is due to G. Birkhoff. Let $\mathfrak{M}$ be a variety of algebras. A subclass $\mathfrak{N}$ in $\mathfrak{M}$ is a (sub)variety if and only if there exists a set of identities (u_i, v_i), $i \in I$, such that $\mathfrak{N}$ consists of all algebras of $\mathfrak{M}$ satisfying these identities. Here u_i, v_i $(i \in I)$ are elements of $F_{\mathfrak{M}}$ with a countable set X of free generators. A variety of algebras is called homogeneous if it is defined by a set of homogeneous identities. For more details about varieties of algebras, we refer to [25, 79, 143, 178].

A variety of algebras is said to be Schreier if any subalgebra of a free algebra of this variety is free in the same variety of algebras; this notion came from group theory. In the 1920s, J. Nielsen [294] and O. Schreier [329] proved that any subgroup of a free group is free. A. G. Kurosh proved in [195] that subalgebras of free nonassociative algebras are free. A. I. Shirshov [345] showed that the variety of Lie algebras is Schreier (this result was also obtained by E. Witt in [403], and he also proved that the variety of all Lie p-algebras is Schreier). A. G. Kurosh in [197] extended this result to the variety of all Ω-algebras. An Ω-algebra is a vector space with a family Ω of basic multilinear multiplications of varieties at least 2. In this paper, he also classified subalgebras of free products of Ω-algebras. Earlier, for the case of all nonassociative algebras it was done in [196], and for the case of all commutative and all anticommutative algebras it was done in [139]. Yu. A. Bahturin [30, 31] and M. V. Zaicev [414] proved that Schreier varieties of Lie algebras are the variety of all Lie algebras and the variety of abelian Lie algebras, respectively. A. I. Shirshov showed in [346] that subalgebras of free nonassociative commutative and anticommutative algebras are free; that is, the varieties of commutative and anticommutative algebras are Schreier.

A. A. Mikhalev in [243] and A. S. Shtern in [369] showed that the variety of Lie superalgebras is Schreier. A. A. Mikhalev proved this result for the variety of color Lie p-superalgebras in [245]. Up to now there is no complete classification of Schreier varieties of algebras. U. U. Umirbaev [388, 392]

obtained new examples of Schreier varieties of algebras and gave necessary and sufficient conditions for a variety of algebras to be Schreier. As for subalgebras of free algebras of varieties of linear Ω-algebras, see articles [26, 38].

Let K be a field, X a set, and let $F = F(X)$ be the free algebra of a homogeneous variety of algebras with the set X of free generators over the field K. For $u \in F(X)$, by $\ell(u) = \ell_X(u)$ we denote the degree of u. Consider also a generalized degree function $\mu\colon X \to \mathbb{N}$, where $\mathbb{N}$ is the set of positive integers. Let $\Gamma(X)$ be the free groupoid of nonassociative monomials in the alphabet X, $S(X)$ the free semigroup of associative words in X, and $^\sim\colon \Gamma(X) \to S(X)$ the bracket removing homomorphism. We set $\mu(x_1 \dots x_n) = \sum_{i=1}^n \mu(x_i)$ for $x_i \in X$. If $\mu(x) = 1$ for all $x \in X$, then μ is just the usual degree, $\mu = \ell$. If $a \in F$, $a = \sum \alpha_i a_i$, $0 \neq \alpha_i \in K$, a_i are basic monomials, $a_j \neq a_s$ with $j \neq s$, then we set $\mu(a) = \max_i\{\mu(\tilde{a}_i)\}$. By a° we denote the leading part of a: $a^\circ = \sum_{j,\mu(a_j)=\mu(a)} \alpha_j a_j$.

A subset M of F is called independent if M is a set of free generators of the subalgebra of F generated by M. A subset $M = \{a_i\}$ of nonzero elements of F is called reduced if for any i the leading part a_i° of the element a_i does not belong to the subalgebra of F generated by the set $\{a_j^\circ \mid j \neq i\}$.

Let $S = \{s_\alpha \mid \alpha \in I\}$ be a subset of F. A mapping $\omega\colon S \to S' \subseteq A$ is an elementary transformation of S if either ω is a nonsingular linear transformation of S, or $\omega(s_\alpha) = s_\alpha$ for all $\alpha \in I$, $\alpha \neq \beta$, and $\omega(s_\beta) = s_\beta + f(\{s_\alpha \mid \alpha \neq \beta\})$, where f is an element of a free algebra of the same variety of algebras. It is clear that elementary transformations of free generating sets induce automorphisms of the algebra F; such automorphisms are called elementary.

Let A be a free algebra of a homogeneous Schreier variety of algebras. One can transform any finite set of elements of the algebra A to a reduced set by using a finite number of elementary transformations and possibly cancelling zero elements. Every reduced subset of the algebra A is an independent subset (this is what is called the Nielsen property). Moreover, by using Kurosh's method, one can construct a reduced set of generators for any subalgebra of the free algebra A. Indeed, let B be a subalgebra of A, $M = \bigcup_{j=0}^\infty M_j$, where M_j consists of G-homogeneous elements of degree j, if nonempty. We set $M_0 = \varnothing$. Then, by induction, we suppose that $M_0, \dots, M_i$ have been defined. Let B_i be the subalgebra of B generated by $\bigcup_{j=0}^i M_j$ and $S_i = \{b \in B_i \mid \ell(b) \leq i+1\}$. Consider the G-homogeneous subsets of $\{b \in B \mid \ell(b) = i+1\}$ that are linearly independent modulo the subspace S_i, and let M_{i+1} be a maximal such subset. It is clear that M generates the subalgebra B. Moreover, M is a reduced set.

Hence any subalgebra of A is free in the same variety of algebras (this is what is called the Schreier property). In [212], J. Lewin proved that for a homogeneous variety of algebras, the Nielsen and Schreier properties are equivalent. By using this equivalence, it is easy to see that automorphism

groups of the corresponding free algebras (of finite rank) are generated by elementary automorphisms (this result was obtained for free Lie algebras by P. M. Cohn in [77] and for free nonassociative algebras by J. Lewin in [212]).

Let $\mathfrak{M}$ be a homogeneous variety of linear algebras over a field K. Let C be an algebra of the variety $\mathfrak{M}$ and $\langle y\rangle$ the free algebra of rank 1 of the variety $\mathfrak{M}$. We consider the free product $B = \langle y\rangle * C \in \mathfrak{M}$. By B_1 we denote the subspace of elements of B with degree 1 with respect to y. Then B_1 is a free one-generated C-bimodule in $\mathfrak{M}$. Consider $C \oplus B_1$ with the multiplication given by

$$(a_1 + m_1)(a_2 + m_2) = a_1a_2 + a_1m_2 + m_1a_2,$$

where $a_1, a_2 \in C$, $m_1, m_2 \in B_1$. We have $C \oplus B_1 \in \mathfrak{M}$. For $a \in C$, by l_a and r_a we denote the universal operators of left and right multiplication, respectively,

$$b \cdot l_a = ab, \quad b \cdot r_a = ba, \quad b \in B_1.$$

Let $U(C) = U_{\mathfrak{M}}(C)$ be the subalgebra of the algebra $\mathrm{End}_F(B_1)$ of endomorphisms of the module B_1 generated by the set $\{1, l_a, r_a \mid a \in C\}$. If the algebra C has the unit element, then we set $r_1 = l_1 = 1$ in $U(C)$. The algebra $U(C)$ is the universal multiplicative enveloping algebra of C. The notion of a C-bimodule in the variety $\mathfrak{M}$ is equivalent to the notion of a right $U(C)$-module; see [157].

By $A = F_{\mathfrak{M}}\langle X\rangle$ we denote the free algebra of the variety $\mathfrak{M}$ with the set $X = \{x_1, \ldots, x_n\}$ of free generators. Let $\mathfrak{M}_0$ be the variety of all algebras and $\Gamma(X)$ the free groupoid of nonassociative monomials (free Magma) without unity element on the alphabet X; i.e., $X \subseteq \Gamma(X)$. If $u, v \in \Gamma(X)$, then $u \cdot v \in \Gamma(X)$, where $u \cdot v$ is the formal multiplication on nonassociative monomials. We consider the linear space $F(X)$ over K with the basis consisting of 1 and the elements of $\Gamma(X)$ with the multiplication given by

$$(\alpha a) \cdot (\beta b) = (\alpha\beta)(a \cdot b)$$

for all $\alpha, \beta \in K$, $a, b \in \Gamma(X)$. The algebra $F(X)$ is the free nonassociative algebra (the free algebra of the variety $\mathfrak{M}_0$). Let $W_0 = \Gamma(X)$, $A = F(X)$. Then the algebra $U(A)$ is the free associative algebra with the set $S_0 = \{r_w, l_w \mid w \in W_0\}$ of free generators (for the details, see [140, 388]).

Let $\mathfrak{M}_1$ be the variety of all commutative algebras, I the two-sided ideal of the free nonassociative algebra $F(X)$ generated by the set $\{ab - ba \mid a, b \in F(X)\}$. Then the factor algebra $A = F(X)/I$ is the free algebra of the variety $\mathfrak{M}_1$ with the set X of free generators (i.e., the free commutative nonassociative algebra).

Suppose that the set $\Gamma(X)$ is totally ordered in such a way that, for $a, b \in \Gamma(X)$, if $\ell(a) > \ell(b)$, then $a > b$ ($\ell(u)$ denotes the degree of a monomial $u \in \Gamma(X)$). We construct the set W_1 of all commutative regular monomials inductively in the following way. First of all, $X \subset W_1$. Furthermore, $w \in W_1$

if $w = uv$, u and v are commutative regular monomials, and $u \leq v$. Then W_1 is a linear basis of $A = F(X)/I$ ([346]). The universal multiplicative enveloping algebra $U(A)$ is the free associative algebra with the set $S_1 = \{r_w \mid w \in W_1\}$ of free generators [140, 388].

Let $\mathfrak{M}_2$ be the variety of all anticommutative algebras and J the two-sided ideal of the free nonassociative algebra $F^+(X)$ without unit element generated by the set $\{aa \mid a \in F(X)\}$. Then the factor algebra $A = F^+(X)/J$ is the free algebra of the variety $\mathfrak{M}_2$ with the set X of free generators (i.e., the free anticommutative nonassociative algebra). We construct the set W_2 of all anticommutative regular monomials inductively: $X \subset W_2$; $w \in W_2$ if $w = uv$, u, and v are anticommutative regular monomials, and $u < v$. Then W_2 is a linear basis of $A = F(X)/J$ ([346]). The universal multiplicative enveloping algebra $U(A)$ is the free associative algebra with the set $S_2 = \{r_w \mid w \in W_2\}$ of free generators [140, 388].

Let G be an abelian semigroup, K a field of characteristic different from two, and $\varepsilon\colon G \times G \to K^*$ a skew symmetric bilinear form (a commutation factor, or a bicharacter); that is,

$$\varepsilon(g,h)\,\varepsilon(h,g) = 1,$$
$$\varepsilon(g_1+g_2,h) = \varepsilon(g_1,h)\,\varepsilon(g_2,h), \quad \varepsilon(g,h_1+h_2) = \varepsilon(g,h_1)\,\varepsilon(g,h_2)$$

for all $g, g_1, g_2, h, h_1, h_2 \in G$;

$$G_- = \{g \in G \mid \varepsilon(g,g) = -1\}, \quad G_+ = \{g \in G \mid \varepsilon(g,g) = +1\}.$$

For instance, if $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $K = \mathbb{C}$, $f = (f_1, f_2), g = (g_1, g_2) \in G$, then the following form is a commutation factor on G: $\varepsilon(f,g) = (-1)^{(f_1+f_2)(g_1+g_2)}$; $G_+ = \{(0,0),(1,1)\}$, $G_- = \{(0,1),(1,0)\}$. Suppose that $n = 2^k$, $k \geq 1$. Let ε_n be a primitive root of 1, $\varepsilon_n = e^{2\pi i/n}$, $G = \langle f\rangle_n \oplus \langle g\rangle_n$ the direct sum of cyclic groups of order n generated by f and g, respectively, $\varepsilon(f,f) = 1$, $\varepsilon(f,g) = \varepsilon_n$, $\varepsilon(g,g) = -1$. Then ε is a commutation factor on G.

M. Scheunert [326] classified all commutation factors on groups $\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$, where p is a prime number. A commutation factor ε on an abelian group G is said to be nondegenerated if $\{g \in G \mid \varepsilon(g,h) = 1\ \forall h \in G\} = \{0\}$. A commutation factor ε' on a group G' is equivalent to a commutation factor ε'' on a group G'' if there is an isomorphism $\varphi\colon G' \to G''$ such that $\varepsilon'(g,h) = \varepsilon''(\varphi(g),\varphi(h))$ for all $g, h \in G'$. A. A. Zolotykh [419] obtained a classification (up to an equivalence) of all nondegenerate commutation factors on finite abelian groups.

A G-graded K-algebra $R = \bigoplus_{g\in G} R_g$ is a color Lie superalgebra if

$$[x,y] = -\varepsilon(d(x),d(y))[y,x], \quad [v,[v,v]] = 0,$$
$$[x,[y,z]] = [[x,y],z] + \varepsilon(d(x),d(y))[y,[x,z]]$$

with $d(v) \in G_-$ for G-homogeneous elements $x, y, z, v \in R$, where $d(a) = g$ if $a \in R_g$. The homogeneous elements of the components R_g, $g \in G_+$, are said to be even, and the homogeneous elements of the components R_g,

$g \in G_-$, are said to be odd. Let $R_+ = \bigoplus_{g \in G_+} R_g$, $R_- = \bigoplus_{g \in G_-} R_g$. We consider only G-homogeneous elements, homomorphisms preserving the G-graded structure, etc.

If $G = \mathbb{Z}_2$ and $\varepsilon(f,g) = (-1)^{fg}$, then a color Lie superalgebra is a Lie superalgebra. If $\varepsilon \equiv 1$, then we have a G-graded Lie algebra (if $G = \{e\}$, then we have a Lie algebra).

We denote $(\operatorname{ad} a)(b) = [a,b] = (a)\operatorname{Ad} b$ for all $a, b \in R$. Let $\operatorname{char} K = p > 2$. A color Lie superalgebra R over K is a color Lie p-superalgebra if on G-homogeneous components R_g, $g \in G_+$, we have a mapping $x \to x^{[p]}$, $d(x^{[p]}) = pd(x)$, such that, for all $\alpha \in K$ and all G-homogeneous elements $x, y, z \in R$ with $d(x) = d(y) \in G_+$, the following conditions are satisfied:

$$(\alpha x)^{[p]} = \alpha^p x^{[p]}, \quad (\operatorname{ad}(x^{[p]}))(z) = [x^{[p]}, z] = (\operatorname{ad} x)^p(z),$$
$$(x+y)^{[p]} = x^{[p]} + y^{[p]} + \sum s_j(x,y),$$

where $js_j(x,y)$ is the coefficient on t^{j-1} in the polynomial $(\operatorname{ad}(tx + y))^{p-1}(x)$.

If Q is a G-graded associative algebra over K, then $[Q]$ denotes the color Lie superalgebra with the operation $[\,,\,]$ where $[a,b] = ab - \varepsilon(d(a),d(b))ba$ for G-homogeneous elements $a, b \in Q$.

If $\operatorname{char} K = p > 2$, and $x^{[p]} = x^p$ for all G-homogeneous elements x of Q with $d(x) \in G_+$, then $[Q]$ with the operation $[p]$ is a color Lie p-superalgebra denoted by $[Q]^p$.

Let $X = \{x_1, \ldots, x_n\} = \bigcup_{g \in G} X_g$ be a G-graded set (that is, $X_g \cap X_f = \varnothing$ for $g \neq f$, $d(x) = g$ for $x \in X_g$), and let $K\langle X\rangle$ be the free G-graded associative K-algebra and $L(X)$ the subalgebra of $[K\langle X\rangle]$ generated by X. Then $L(X)$ is the free color Lie superalgebra with the set X of free generators. In the case where $\operatorname{char} K = p > 2$, let $L^p(X)$ be the subalgebra of $[K\langle X\rangle]^p$ generated by X. Then $L^p(X)$ is the free color Lie p-superalgebra on X. For more information on free Lie superalgebras, we refer to the monographs [33, 275].

We combine the main properties of free algebras of main types of Schreier varieties of algebras in one theorem.

Theorem 11.1.1 ([77, 195, 212, 243, 244, 245, 345, 346, 369, 403]). *Let X be a finite set, $X = \{x_1, \ldots, x_n\}$, K a field, $\operatorname{char} K \neq 2$, $F = F(X)$ the free algebra without the unity element on the set X of free generators of one of the following varieties of algebras over a field K: the variety of all algebras, the variety of Lie algebras, varieties of color Lie superalgebras, the variety of Lie p-algebras, varieties of color Lie p-superalgebras, or varieties of commutative and anticommutative algebras.*

1. *Any finite subset of F can be transformed into a reduced subset by a finite sequence of elementary transformations (with cancellation of possible zeros).*

2. *Any reduced subset of the algebra F is an independent subset.*

3. *The leading part of a polynomial on a reduced subset is a polynomial on leading parts of elements of this subset.*

4. *Any subalgebra of F is free.*

5. *A subset M of F is independent if and only if it is linearly independent modulo the square of the subalgebra of F generated by M (for free color Lie p-superalgebras, we add to the square the ideal all p-powers of elements of M).*

6. *If $|X| < \infty$, then the automorphism group of F is generated by elementary automorphisms.*

Problem 11.1.2 (P. M. Cohn [77]). Is it true that the automorphism group of a free associative algebra of finite rank is generated by elementary automorphisms?

Note that this problem has a positive solution for both polynomial algebra in two variables (H. W. E. Jung [164], W. van der Kulk [194]) and the free associative algebra of rank 2 (A. J. Czerniakiewicz [86], L. G. Makar-Limanov [233]).

Let $X = \{x_1, \ldots, x_n\}$. It follows from Theorem 11.1.1 that free algebras $F(X)$ are Hopfian; that is, if the algebra $F(X)$ is generated by elements $u_1, \ldots, u_n$, then these elements form a free generating set of $F(X)$.

11.2 Schreier Techniques

O. Schreier [329] introduced very useful techniques to obtain free generators for a subgroup of a free group from a special set of coset representatives. Later, this technique was extended by many authors for different types of free algebras.

Subalgebras of the free associative algebra are not necessarily free. For example, if we consider elements x^2 and x^3 in the free associative algebra $K\langle x\rangle$, then $x^2x^3 = x^3x^2$. Hence the subalgebra generated by x^2 and x^3 is not free. At the same time, we have P. M. Cohn's result that over a free associative algebra submodules of free left modules are free. P. M. Cohn obtained this result using a generalization of the Euclidean algorithm in the free associative algebra.

Let K be a field. The family $\{a_i \mid i \in I\}$ of elements of the free associative algebra $K\langle X\rangle$ is called left ℓ-dependent if there exist elements $b_i \in K\langle X\rangle$, almost all zero, such that

$$\ell\Big(\sum_i b_i a_i\Big) < \max\{\ell(a_i) + \ell(b_i)\}$$

or if some a_i is equal to zero. Otherwise the family $\{a_i\}$ is called left ℓ-independent.

An element $a \in K\langle X\rangle$ is said to be left ℓ-dependent on a family $\{a_i\}$ if either $a_i = 0$ or there exist $b_i \in K\langle X\rangle$, almost all zero, such that

$$\ell\Big(a - \sum_i b_i a_i\Big) < \ell(a), \quad \ell(a_i) + \ell(b_i) \le \ell(a)$$

for all i. Otherwise a is said to be left ℓ-independent on a family $\{a_i\}$.

In the free associative algebra over a field K, the following analog of the Euclidean algorithm takes place:

Theorem 11.2.1 (weak algorithm [74, 75]). *Let $a_1, \dots, a_n \in K\langle X\rangle$ and $\ell(a_1) \le \dots \le \ell(a_n)$. Then, if the family $\{a_1, \dots, a_n\}$ is left ℓ-dependent, there exists i, $1 \le i \le n$, such that the element a_i is left dependent on the family $\{a_1, \dots, a_{i-1}\}$.*

Note that the right version of this algorithm also takes place in $K\langle X\rangle$.

Since the weak algorithm takes place in $K\langle X\rangle$, the algebra $K\langle X\rangle$ is a free ideal ring (a fir) — i.e., $K\langle X\rangle$ is left fir and right fir; that is, left (right) ideals of $K\langle X\rangle$ are free left (right, respectively) $K\langle X\rangle$-modules of unique rank. Moreover, in a left fir every submodule of a free left module is free [76, 80].

Note that a very elegant proof of this fact is given by P. M. Cohn's theorem that the free product of firs is again fir. In [213] J. Lewin, with the use of Schreier's technique, gave a direct proof of the fact that $K\langle X\rangle$ is a fir.

Using the weak algorithm, P. M. Cohn [77] obtained the following sufficient condition for a subalgebra of a free algebra to be free. Let B be a subalgebra of $K\langle X\rangle$. We consider $K\langle X\rangle$ as a left B-module relative to usual multiplication. A system of elements $S = \{s_i \mid i \in I\}$ of $K\langle X\rangle$ is said to be B-independent if for almost all zero elements a_i

$$\ell\Big(\sum_i a_i s_i\Big) = \max\{\ell(v_i) + \ell(s_i)\}.$$

Theorem 11.2.2 ([77]). *If B is any subalgebra of $K\langle X\rangle$ such that $K\langle X\rangle$ is free as a left B-module, with a B-independent basis, then B is a free associative algebra over K. In particular, if B is a subalgebra of $K\langle X\rangle$ such that $K\langle X\rangle$ satisfies the weak algorithm as a B-module, then B is a free subalgebra of $K\langle X\rangle$.*

For more information on free ideal rings, we refer to P. M. Cohn's monograph [80].

Suppose that F is a free group of rank n, and let $H \subset F$ be a subgroup of a finite index. Then H is also the free group; moreover, the rank m of H is determined by Schreier's well-known formula [329]: $m-1 = (n-1)\cdot|F : H|$.

J. Lewin [213] obtained the following analog of Schreier's formula for free associative algebras. For a left ideal M of $K\langle X\rangle$, we denote by $\operatorname{rank}(M)$ the rank of the free left $K\langle X\rangle$-module M.

Theorem 11.2.3 ([213]). *Let $|X| = n$ and let I be a left ideal of $K\langle X\rangle$ such that $\dim_K(K\langle X\rangle/I) = k < \infty$. Then I is a free left $K\langle X\rangle$-module, $\operatorname{rank}(I) = k(n-1)+1$.*

For free Lie p-algebras, G. P. Kukin [192] obtained the following analog of Schreier's formula.

Theorem 11.2.4 ([192]). *Let K be a field, $p = \operatorname{char} K > 2$, $|X| = N < \infty$. Suppose that H is a subalgebra of the free Lie p-algebra $L^p(X)$, $\dim L^p(X)/H = t < \infty$. Then $\operatorname{rank}(H) = p^t(N-1)+1$.*

A. A. Mikhalev [243, 244, 245] obtained Schreier-type formulas for free Lie superalgebras and p-superalgebras.

Theorem 11.2.5 ([243]). *Let K be a field, $\operatorname{char} K \neq 2, 3$, $L = L(X) = L_+ \oplus L_-$ the free color Lie superalgebra, $\operatorname{rank}(L) = |X| = N < \infty$, and let H be a G-homogeneous subalgebra of L, $H = H_+ \oplus H_-$, $H_+ = L_+$, $\dim(L_-/H_-) = s < \infty$. Then $\operatorname{rank}(H) = 2^s(N-1)+1$.*

Theorem 11.2.6 ([245]). *Let K be a field, $p = \operatorname{char} K > 3$, $|X| = N < \infty$. Suppose that $H = H_+ \oplus H_-$ is a G-homogeneous subalgebra of the free color Lie p-superalgebra $L^p(X)$, $\dim(L_+^p/H_+) = t < \infty$, and $\dim(L_-^p/H_-) = s < \infty$. Then $\operatorname{rank}(H) = 2^s p^t(N-1)+1$.*

A. A. Mikhalev showed that any subalgebra of finite rank of $L(X)$ is completely defined by its (nontrivial) even component.

Theorem 11.2.7 ([33, 275]). *Let K be a field, $\operatorname{char} K \neq 2, 3$, $|X_-| \geq 1$, and let A, B be G-homogeneous subalgebras of finite rank in the free color Lie superalgebra $L(X)$, $A = A_+ \oplus A_-$, $B = B_+ \oplus B_-$. If $A_- = B_- \neq \{0\}$, then $A = B$.*

In the study of subalgebras of free algebras, the elimination of variables plays a very important role.

Let $x \in X$, $v \in X_+$, and $z \in X_-$, where $X_+ = \bigcup_{g\in G_+} X_g$, $X_- = \bigcup_{g\in G_-} X_g$. We denote

$$Z(x) = \{y, y(\operatorname{Ad} x)^n \mid y \in X \setminus \{x\},\ n \in \mathbb{N}\} \subset L(X);$$
$$ZP(v) = \{y, v^p, y(\operatorname{Ad} v)^n \mid y \in X \setminus \{x\},\ n = 1, \ldots, p-1\} \subset L^p(X);$$
$$W(z) = \{y, [y,z], [z,z] \mid y \in X \setminus \{x\}\} \subset L(X).$$

For free Lie algebras, the elimination theorem was obtained by M. Lazard [202].

Theorem 11.2.8 ([202]). *Let $L(X)$ be the free Lie algebra, $x \in X$. Then $Z(x)$ is an independent subset of $L(X)$ and*

$$L(X) = Kx \oplus L(Z(x)).$$

W. Magnus [230] obtained elimination theorems for free associative rings. Elimination of variables in free color Lie superalgebras and p-superalgebras was considered by A. A. Mikhalev.

Theorem 11.2.9 ([243, 244, 245, 33, 275]).

1. *Let $L(X)$ be the free color Lie superalgebra, $x \in X$, $z \in X_-$. Then $Z = Z(x)$ and $W = W(z)$ are independent subsets of $L(X)$. The ideal of $L(X)$ generated by $\{y \in X \mid y \neq x\}$ is equal to $L(Z(x))$. Moreover, $L(X) = L(x) \oplus L(Z(x))$ is a semidirect product of the free algebras $L(x)$ and $L(Z(x))$ with the adjoint action of $L(x)$ on $L(Z(x))$. We also have $L(X) = Kz \oplus L(W(z))$ as vector spaces.*

2. *Let $L^p(X)$ be the free color Lie superalgebra, $x \in X$, $v \in X_+$, $z \in X_-$. Then $Z(x)$, $ZP(v)$, and $W(z)$ are independent subsets of $L^p(X)$. Moreover, $L^p(X) = L^p(x) \oplus L^p(Z(x))$ is a semidirect product with the adjoint action and $L^p(X) = Kv \oplus L^p(ZP(v))$, $L^p(X) = Kz \oplus L^p(W(z))$ as vector spaces.*

The elimination theorem for free Lie superalgebras was obtained also by J. Désarménien, G. Duchamp, D. Krob, and G. Melançon [91]. Recently N. Dobrynin [98, 99] obtained some generalizations of the elimination theorem for free Lie superalgebras. For free partially commutative Lie algebras elimination theorems were obtained by G. Duchamp and D. Krob [114], and for free partially commutative superalgebras — by N. Dobrynin [98, 99].

Note that a straightforward analog of Schreier's formula for the free Lie algebras does not exist. It is well-known that the rank of a subalgebra of finite codimension of a free Lie algebra is infinite; see, for example, [32]. But recently V. M. Petrogradsky found a form of Schreier's type formula for free Lie algebras and superalgebras in terms of formal power series [303, 305, 99]. He also established versions of the Schreier formula for these algebras using exponential generating functions (complexity functions) [302]. Recently he obtained Schreier formulas for free nonassociative algebras and free commutative and anticommutative nonassociative algebras [306]. We illustrate here his idea for free Lie algebras.

Let X be at most a countable set with a weight function $\mathrm{wt}\colon X \to \mathbb{N}$ (where $\mathbb{N}$ is the set of positive integers) such that

$$X = \bigcup_{i=1}^{\infty} X_i, \quad X_i = \{x \in X \mid \mathrm{wt}\, x = i\}; \quad |X_i| < \infty, \quad i \in \mathbb{N}.$$

We call such a set finitely graded. For any monomial $y = x_{i_1} \dots x_{i_n}$, $x_{i_j} \in X$, we set $\mathrm{wt}\, y = \mathrm{wt}\, x_{i_1} + \dots + \mathrm{wt}\, x_{i_n}$. Suppose that Y is a set of monomials

in X. Then we denote $Y_i = \{y \in Y \mid \operatorname{wt} y = i\}$, $i \in \mathbb{N}$. Also, we define the Hilbert–Poincaré series of Y as $\mathcal{H}_X(Y,t) = \sum_{i=1}^{\infty} |Y_i| t^i$.

Let $A = A(X)$ be an algebra generated by a finitely graded set X, and suppose that A inherits the gradation from X. Let $V \subset A$ be a homogeneous subspace; that is, $V = \bigoplus_{i=1}^{\infty} V_i$ with $V_i = \{v \in V \mid \operatorname{wt} v = i\}$. We define the Hilbert–Poincaré series of V as $\mathcal{H}_X(V,t) = \sum_{i=1}^{\infty} \dim(V_i) t^i$. We sometimes omit t, X and write $\mathcal{H}(Y)$, $\mathcal{H}(V)$.

Now let $Y \subset A$ be a not necessarily homogeneous subset. For $v \in A$, consider its decomposition into homogeneous components $v = v_1 + \cdots + v_n$, $\operatorname{wt}(v_i) = i$, $i = 1, \ldots, n$, $v_n \neq 0$. In this case, we write $\deg(v) = n$, $\operatorname{gr}(v) = v_n$. We define

$$\mathcal{H}_X(Y,t) = \sum_{n=1}^{\infty} |Y_n| t^n, \quad \text{where} \quad Y_n = \{y \in Y \mid \deg(y) = n\}.$$

Given a subspace $V \subset A$, one has a filtration $0 = V^0 \subset V^1 \subset \ldots$ with $V^i = \{v \in V \mid \deg(v) \leq i\}$, $i = 0, 1, 2, \ldots$. Let $\operatorname{gr}(V) = \bigoplus_{n=1}^{\infty} \operatorname{gr}_n(V)$, where

$$\operatorname{gr}_n(V) = \{\operatorname{gr}(v) \mid v \in V, \ \deg(v) = n\} \cup 0 \equiv V^n / V^{n-1}$$

denote the associated graded space. In the nonhomogeneous case, the Hilbert–Poincaré series is defined as follows:

$$\mathcal{H}_X(V,t) = \mathcal{H}(\operatorname{gr} V, t) \quad = \sum_{n=1}^{\infty} \dim_K(\operatorname{gr}_n(V)) t^n;$$

$$\mathcal{H}_X(A/V,t) = \mathcal{H}(A/\operatorname{gr} V, t) = \sum_{n=1}^{\infty} \dim_K(A_n \operatorname{gr}_n(V)) t^n.$$

We consider all series as elements of the ring of the formal power series

$$\mathbb{Z}[[t]] = \left\{ \sum_{n=0}^{\infty} b_n t^n \mid b_n \in \mathbb{Z} \right\}.$$

By $\mathbb{Z}_0[[t]]$ we denote a set of series with $b_0 = 0$. We consider the operator $\mathcal{E} \colon \mathbb{Z}_0[[t]] \to \mathbb{Z}[[t]]$

$$\mathcal{E} \colon \varphi(t) = \sum_{n=1}^{\infty} b_n t^n \to \mathcal{E}(\varphi(t)) = \sum_{n=0}^{\infty} a_n t^n = \prod_{n=1}^{\infty} \frac{1}{(1-t^n)^{b_n}}.$$

Let L be a Lie algebra generated by X, let $U(L)$ be its universal enveloping algebra, and suppose that

$$\mathcal{H}_X(L,t) = \sum_{n=1}^{\infty} b_n t^n, \quad \mathcal{H}_X(U(L),t) = \sum_{n=0}^{\infty} a_n t^n.$$

It is well-known that $\mathcal{H}_X(U(L)) = \mathcal{E}(\mathcal{H}_X(L))$ [384].

Theorem 11.2.10 ([303]). *Let L be a free Lie algebra freely generated by a finitely graded set X. Suppose that H is a subalgebra and Y is the set of free generators for H. Then*

$$\mathcal{H}(Y) - 1 = (\mathcal{H}(X) - 1) \cdot \mathcal{E}(\mathcal{H}(L/H)).$$

For more information on Schreier techniques, we refer to the following articles and monographs: [32, 33, 34, 57, 91, 99, 189, 190, 192, 195, 198, 202, 212, 213, 227, 230, 231, 243, 244, 245, 248, 252, 275, 302, 303, 304, 305, 306, 313, 322, 329, 345, 346, 369, 388, 392, 403, 414].

11.3 Free Differential Calculus

R. H. Fox [134] introduced free differential calculus in free group rings; see Section 1.4. Let $F = F(X)$ be the free group on a set X, $\mathbb{Z}F$ the integral group ring of F, and Δ_F the augmentation ideal of $\mathbb{Z}F$ (i.e., the kernel of the natural homomorphism

$$\sigma\colon \mathbb{Z}F \to \mathbb{Z}, \quad \sigma\Big(\sum_i (n_i f_i)\Big) = \sum_i n_i,$$

where $n_i \in \mathbb{Z}$, $f_i \in F$). The Fox partial derivation with respect to x_i is a mapping $d_i\colon \mathbb{Z}F \to \mathbb{Z}F$ that satisfies the following conditions:

$$\begin{aligned} d_i(x_j) &= \delta_{ij}, \\ d_i(uv) &= u d_i(v) + \sigma(v)\, d_i(u), \\ d_i(ku + lv) &= k d_i(u) + l d_i(v), \end{aligned}$$

$u, v \in \mathbb{Z}F$, $k, l \in \mathbb{Z}$.

There is another interpretation of d_i as follows. The ideal Δ_F is a free left $\mathbb{Z}F$-module with a free basis $\{(x_i - 1) \mid 1 \le i \le n\}$, and the mappings d_i are projections to the corresponding free cyclic direct summands. Every element $u \in \Delta_F$ can be uniquely written in the form

$$u = \sum_{i=1}^{n} d_i(u)(x_i - 1).$$

11.3.1 Free differential calculus and Schreier varieties

As before, by $A = F_{\mathfrak{M}}\langle X\rangle$ we denote the free algebra of the variety $\mathfrak{M}$ with the set $X = \{x_1, \dots, x_n\}$ of free generators.

Let I_A be a free right $U(A)$-module with a basis $y_1, \dots, y_n$,

$$I_A = y_1 U(A) \oplus \cdots \oplus y_n U(A).$$

The linear mapping $\mathcal{D}\colon A \to I_A$ given by $\mathcal{D}(x_i) = y_i$, $1 \le i \le n$,

$$\mathcal{D}(ab) = \mathcal{D}(a) \cdot r_b + \mathcal{D}(b) \cdot l_a,$$

$a, b \in A$, is called the universal derivation of the algebra A in the variety $\mathfrak{M}$. The partial derivatives $\frac{\partial f}{\partial x_i}$ of an element f of A are uniquely determined by

$$\mathcal{D}(f) = \sum_{i=1}^{n} y_i \frac{\partial f}{\partial x_i}.$$

We set

$$\partial(f) = \left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} \right)^{\mathrm{T}},$$

where T is the operator of transposition. From the definition, we get $\frac{\partial}{\partial x_i}(x_j) = \delta_{ij}$, the Kronecker symbol,

$$\frac{\partial}{\partial x_i}(uv) = \frac{\partial u}{\partial x_i} r_v + \frac{\partial v}{\partial x_i} l_u, \quad u, v \in A. \tag{11.1}$$

For a subalgebra H of the algebra A by J_H, we denote the $U(A)$-submodule of the module I_A generated by the elements $D(h)$, $h \in H$. A variety $\mathfrak{M}$ has the property of differential separability for subalgebras if for any subalgebra H of A and $a \in A$, $D(a) \in J_H$ if and only if $a \in H$.

Theorem 11.3.1. *The following varieties have the property of differential separability for subalgebras:*

1. *the variety of all algebras;*
2. *the variety of all commutative algebras* ($\operatorname{char} K \neq 2$);
3. *the variety of all anticommutative algebras;*
4. *the varieties of Lie (super)algebras and p-(super)algebras;*
5. *the variety of algebras with zero multiplication.*

The first time the property of differential separability for subalgebras for Lie algebras was mentioned was in [385] (for Lie superalgebras, see [249]). In general form, this theorem was proved by U. U. Umirbaev in [388].

For Lie algebras and superalgebras, the property of differential separability for subalgebras follows from the Poincaré–Birkhoff–Witt theorems.

Let L be a color Lie superalgebra, U a G-graded associative K-algebra with 1, and $\delta\colon L \to [U]$ a homomorphism of color Lie superalgebras. We say that the algebra U (with δ) is the universal enveloping algebra of L (we denote it $U(L)$) if for any homomorphism σ of the color Lie superalgebra L into a color Lie superalgebra $[R]$ (with the same ε and G) for some G-graded associative algebra R with 1 there exists a unique homomorphism $\theta\colon U \to R$ of G-graded associative algebras with 1 such that $\sigma = \theta\delta$. Let K be a field, $p = \operatorname{char} K > 2$, L a color Lie p-superalgebra, and U a G-graded associative K-algebra with 1, $\delta\colon L \to [U]^p$ a homomorphism of color Lie p-superalgebras. We say that U (with δ) is the restricted universal enveloping

algebra of L (notation $u(L)$) if for any homomorphism $\sigma\colon L \to [R]^p$ of color Lie p-superalgebras, where R is a G-graded associative K-algebra with 1 (with the same ε and G), there exists a unique homomorphism $\theta\colon U \to R$ of G-graded associative K-algebras with 1 such that $\sigma = \theta\delta$. Suppose now that L is a color Lie superalgebra with a G-homogeneous basis $X = X_+ \cup X_-$, $K\langle X\rangle$ is the free G-graded associative algebra, and I is the two-sided ideal in $K\langle X\rangle$ generated by the elements of the form $ab - \varepsilon(d(a), d(b))\, ba - [a, b]$ for all homogeneous $a, b \in L$. Consider the canonical mapping $\delta\colon L \to K\langle X\rangle/I = U(L)$. It is clear that $U(L)$ is the universal enveloping algebra of L. Let $\leq$ be a total ordering of X.

Theorem 11.3.2 (PBW type). *The universal enveloping algebra $U(L)$ constructed above has a G-homogeneous basis consisting of 1 and all monomials $\delta(x_1)\dots\delta(x_n)$ where $n \in \mathbb{N}$, $x_i \in X$, $x_i \leq x_{i+1}$, $x_i \neq x_{i+1}$ with $x_i \in X_-$ for all $i = 1, \dots, n-1$ (in particular, δ is an embedding).*

Let K be a field, $\operatorname{char} K = p > 2$, L a color Lie p-superalgebra with a G-homogeneous linear basis X, J the two-sided ideal of $K\langle X\rangle$ generated by elements $ab - \varepsilon(d(a)a, d(b))ba - [a, b]$ (where a, b are homogeneous, $a, b \in L$), and $a^p - a^{[p]}$ $(a \in L_g,\ g \in G_+)$. Let $\delta\colon L \to K\langle X\rangle/J$ be the canonical mapping. It is clear that $K\langle X\rangle/J = u(L)$ is the restricted universal enveloping algebra for L.

Theorem 11.3.3 (PBW type). *The monomials $\delta(x_1)^{\lambda_1}\dots\delta(x_n)^{\lambda^n}$, where $x_i \in X$, $x_1 < \dots < x_n$, $0 \leq \lambda_i \leq p-1$ for $x_i \in X_+$, $\lambda_i = 0, 1$ for $x_i \in X_-$ give us a linear basis of $u(L)$.*

It is clear that the universal enveloping algebra of the free color Lie superalgebra $L(X)$ is the free associative algebra $K\langle X\rangle$. This algebra is also the universal multiplicative enveloping algebra of $L(X)$. For the restricted universal enveloping algebra of the free color Lie p-superalgebra $L^p(X)$, we have $u(L^p(X)) = K\langle X\rangle$. This algebra is also the universal multiplicative enveloping algebra of $L^p(X)$. For more results concerning PBW theorems for Lie superalgebras, we refer to the monographs [33, 275, 327].

Theorem 11.3.4. *Let K be a field, L a color Lie superalgebra, and B a subalgebra of L. Then B is differentially separable; i.e., if J is the left ideal of $U(L)$ generated by B, then $L \cap J = B$.*

In the case where $\operatorname{char} K = p > 2$, let M be a color Lie p-superalgebra and D a subalgebra of M. Then D is differentially separable (relative to $u(M)$).

Proof. Let $E = \{e_1, e_2, \dots\}$ be a G-homogeneous ordered K-linear basis of the subalgebra B. We extend the subset E up to a G-homogeneous ordered K-linear basis $E \cup H$ of L such that $H = \{h_1, h_2, \dots\}$ and $h_i < e_j$ for all i, j. By Theorem 11.3.2, the set of all monomials

$$h_{i_1}\dots h_{i_m} \cdot e_{i_1}\dots e_{i_n}$$

where

$$h_{i_1} \leq \cdots \leq h_{i_m}, \quad e_{i_1} \leq \cdots \leq e_{i_n},$$

$i_r \neq i_{r+1}$ with $d(h_{i_r}) \in G_-$, $j_s \neq j_{s+1}$ with $d(e_{j_s}) \in G_-$, gives us a K-linear basis of $K\langle X\rangle$. Since B is a subalgebra of L, these monomials with $n \geq 1$ form a K-linear basis of J. Therefore $L \cap J = B$.

The same arguments work for the color Lie p-superalgebra M (we need only use Theorem 11.3.3). ■

Using the property of differential separability of subalgebras, it is possible to prove that free Lie algebras and superalgebras are residually finite.

Theorem 11.3.5 ([249, 385]). *Let $L(X)$ be a free color Lie superalgebra over a field K (in the case* $\operatorname{char} K = p > 2$*, we consider also a free color Lie p-superalgebra $L^p(X)$). Then the algebra $L = L(X)$ ($L = L^p(X)$, respectively) is residually finite; i.e., if a is a G-homogeneous element of L, B is a G-homogeneous finitely generated subalgebra of L, $a \notin B$, then there exists a finite-dimensional color Lie (p-)superalgebra H and an epimorphism $\varphi\colon L \to H$ such that $\varphi(a) \notin \varphi(B)$.*

Proof. It is sufficient to prove the statement in the case where $|X| < \infty$. At the beginning, we consider the free color Lie superalgebra $L = L(X)$. The free G-graded associative algebra $K\langle X\rangle$ is the universal enveloping algebra of L. Consider the left ideal J of $K\langle X\rangle$ generated by the subalgebra B. Since B is a finitely generated subalgebra, J is a finitely generated left ideal of $K\langle X\rangle$. Since $a \in L$ and $a \notin B$, by Theorem 11.3.4 $a \notin J$. Since the ideal J is finitely generated, there exists a left G-graded ideal J' of finite codimension in $A(X)$ such that $a \notin J'$.

Consider the finite-dimensional left $U(L)$-module $M = U(L)/J'$, where $U(L) = K\langle X\rangle$. Let $\operatorname{Ann}(M)$ be the annihilator of the module M and $R = U(L)/\operatorname{Ann}(M)$. Then R is a finite-dimensional G-graded associative algebra, M is a faithful R-module, and $\operatorname{Ann}(M) \subseteq J'$ since $1 \in U(L)$. Let $\xi\colon U(L) \to R$ be the canonical epimorphism. It is obvious that $H = [\xi(L)]$ is a finite-dimensional color Lie superalgebra. Assuming now that $\xi(a) \in \xi(B)$, one obtains for $\{u_1, \ldots, u_r\}$ a set of generators of the subalgebra B such that $\xi(a)$ belongs to the left ideal of R generated by $\xi(u_1), \ldots, \xi(u_r)$. Therefore there exist elements $v_1, \ldots, v_r \in U(L)$ such that

$$\xi(a) = \sum_{i=1}^{r} \xi(v_i)\,\xi(u_i),$$

in other words

$$a - \sum_{i=1}^{r} \xi(v_i)\,\xi(u_i) \in \operatorname{Ann}(M) \subseteq J',$$

and thus $a \in J'$. This contradiction completes the proof of our theorem in the case $L = L(X)$.

In the case $\operatorname{char} K = p > 2$ and $L = L^p(X)$, the proof is the same using the fact that the free G-graded associative algebra $K\langle X\rangle$ is the restricted universal enveloping algebra of L. ■

In group theory, a well-known theorem by M. Hall shows that free groups are residually finite. G. V. Kryazhovskih [188] showed that free nonassociative algebras and free commutative and anticommutative nonassociative algebras are residually finite. This result for free Lie algebras over fields of positive characteristic and for free restricted Lie algebras was obtained by G. P. Kukin [193]. A similar statement does not hold for free rings. In the review article [126] is the following example, which is due to K. Mandelberg. If F is a free ring on one generator x, then in any homomorphism of F onto a finite ring, the subring B generated by $2x$ and $2x^2 + x$ maps onto the image of F. At the same time $x \notin B$.

The following result by U. U. Umirbaev gives a necessary condition for a variety of algebras to be Schreier.

Theorem 11.3.6 ([388]). *If $\mathfrak{M}$ is a homogeneous Schreier variety of algebras, then*

1. *for any free algebra A of $\mathfrak{M}$ the universal multiplicative enveloping algebra $U(A)$ is a free associative algebra;*
2. *for any homogeneous subalgebra H of a free algebra A of the variety $\mathfrak{M}$ the algebra $U(A)$ is a free right $U(H)$-module.*

If $\operatorname{char} K = 0$, then a variety satisfying conditions 1 and 2 is Schreier.

Point 1 of Theorem 11.3.6 for free nonassociative algebras and for free commutative and anticommutative nonassociative algebras was proved by A. T. Gainov [140].

A method to test that a variety of algebras is Schreier is given by the following theorem.

Theorem 11.3.7 ([388]). *Let $\mathfrak{M}$ be a homogeneous variety of algebras such that:*

1. *For any free algebra A of $\mathfrak{M}$, the universal multiplicative enveloping algebra $U(A)$ is a free associative algebra.*
2. *The variety $\mathfrak{M}$ has the property of differential separability for subalgebras.*

Then $\mathfrak{M}$ is a Schreier variety.

It follows that:

Theorem 11.3.8 ([388]). *The variety of algebras defined by the identity $x \cdot x^2 = 0$ is Schreier.*

Problem 11.3.9. To give the complete classification of Schreier varieties of algebras.

An algebra A over a field K with an anticommutative bilinear operation $[x, y]$ and a trilinear operation $\mathcal{A}(x, y, z)$ is called an Akivis algebra if

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = \mathcal{A}(x, y, z) + \mathcal{A}(y, z, x) + \mathcal{A}(z, x, y) - \mathcal{A}(y, x, z) - \mathcal{A}(x, z, y) - \mathcal{A}(z, y, x).$$

These algebras were introduced by M. A. Akivis as tangent algebras of local analytic groups. I. P. Shestakov and U. U. Umirbaev [338] proved that the variety of Akivis algebras is Schreier, automorphisms of finitely generated free Akivis algebras are tame, the occurrence problem for free Akivis algebras is decidable, finitely generated subalgebras of free Akivis algebras are residually finite, and the word problem is decidable for the variety of Akivis algebras.

For any element a of the free associative algebra $K\langle X\rangle$, we have the unique presentation in the form $a = \alpha \cdot 1 + x_1 a_1 + x_2 a_2 + \ldots$, where only a finite number of elements $a_i \in K\langle X\rangle$ are nonzero, $\alpha \in K$. We call the element a_i the right Fox partial derivative of the element a by x_i, and we use the notation $a_i = \frac{\partial a}{\partial x_i} = \frac{\partial}{\partial x_i} a$. Thus we have the operators $\frac{\partial}{\partial x_i}$. These operators are exactly linear mappings $\frac{\partial}{\partial x_i} \colon K\langle X\rangle \to K\langle X\rangle$ such that $\frac{\partial}{\partial x_i}(x_j) = \delta_{ij}$ and

$$\frac{\partial}{\partial x_i}(uv) = \frac{\partial}{\partial x_i}(u)v + \sigma(u)\frac{\partial}{\partial x_i}(v),$$

where $\sigma \colon K\langle X\rangle \to K\langle X\rangle$ is the homomorphism defined by $\sigma(x_i) = 0$ for all $x_i \in X$. For one of the applications of these derivatives, see Section 9.2.1.

For all $a \in L(X)$ and $b \in K\langle X\rangle$, we set $l_a \cdot b = -\varepsilon(a, b)ba$ and $a \cdot r_b = a \cdot b$. Then $K\langle X\rangle$ is an $L(X)$-bimodule. It is clear that the universal multiplicative enveloping algebra of $L(X)$ is exactly the free G-graded associative algebra $K\langle X\rangle$ with the actions l_a and r_a defined above (at the same time, $K\langle X\rangle$ is the universal enveloping algebra of the color Lie superalgebra $L(X)$). The derivation

$$D \colon L(X) \to I_A = \bigoplus_{i=1}^{n} dx_i \cdot K\langle X\rangle$$

given by

$$D(a) = \sum_{i=1}^{n} dx_i \cdot \frac{\partial a}{\partial x_i}$$

for all $a \in L(X)$ (only a finite number of summands are nonzero) is the universal derivation of $L(X)$.

For more information on Schreier varieties of algebras, we refer to the articles [388, 392] (for the varieties of linear Ω-algebras, see [26, 38]).

Free differential calculus can be applied to a study of free abelian extensions in a variety $\mathfrak{V}$. Let A be an algebra in $\mathfrak{V}$ with a fixed set of

generators X. We say that an algebra B in $\mathfrak{V}$ is a free abelian extension of A in $\mathfrak{V}$ if

1. B is generated by the same set X.
2. There exists a surjective homomorphism $\gamma\colon B \to A$ that is identical on X.
3. If C is an algebra in $\mathfrak{V}$ generated by the set X having a surjective homomorphism $\eta\colon C \to A$ that is identical on X, then there exists a homomorphism $\xi\colon B \to C$ such that $\eta\xi = \gamma$.

Take a free $\mathfrak{V}$-algebra A with the set X of free generators. Since A is generated by the set X, there exists a surjective homomorphism of algebras $\rho\colon F \to A$ that is identical on X. Denote by I the kernel $\ker\rho$. It is not difficult to show that the free abelian extension B is precisely F/I^2, where I^2 is the ideal in F generated by all products ab, $a, b \in I$. Thus, free abelian extensions are analogs of wreath products in group theory. An extension of a study of free abelian extensions to any congruence-modular variety in universal algebra and a development of generalized free differential calculus is exposed in [23].

11.3.2 Ranks of subalgebras

Using free differential calculus (universal derivations), A. A. Mikhalev, V. Shpilrain, and A. A. Zolotykh [257] obtained matrix algorithms to find ranks of subalgebras of free Lie algebras. A. A. Mikhalev and A. A. Zolotykh [279] constructed such algorithms for subalgebras of free Lie superalgebras and free Lie p-superalgebras. Recently, K. Champagnier [67] obtained similar results for ranks of subalgebras of free nonassociative algebras and free (anti)commutative nonassociative algebras.

Let K be a field, $\operatorname{char} K \neq 2$, and $L(X)$ the free color Lie superalgebra (if $\operatorname{char} K = p > 2$, also let $L^p(X)$ be the free color Lie p-superalgebra). For the algebra $A = L(X)$ ($A = L^p(X)$), the universal multiplicative enveloping algebra $U(A)$ of A is the free associative algebra $K\langle X\rangle$. Let $H = \{h_1, \ldots, h_m\}$ be a subset of G-homogeneous elements of A. Consider the matrix $J(H) = (\frac{\partial h_j}{\partial x_i})$, $1 \leq i \leq n$, $1 \leq j \leq m$. Here partial derivatives $\frac{\partial h_j}{\partial x_i}$ are components of the (right) universal derivation. Consider the columns $\partial(h_j)$, $1 \leq j \leq m$, of the matrix $J(H) = (\partial(h_1), \ldots, \partial(h_m))$.

Theorem 11.3.10 ([279]). *A subset $H = \{h_1, \ldots, h_m\}$ of A is independent if and only if the columns of the matrix $J(H)$ are right independent over $U(A)$.*

Theorem 11.3.11 ([279]). *Let $H = \{h_1, \ldots, h_m\} \subset A$. Then the rank of the subalgebra of A generated by H is equal to the rank of the free right $U(A)$-submodule of $U(A)^n$ generated by the columns of the matrix $J(H)$.*

Theorem 11.3.10 gives an effective algorithm to decide whether a given subset of A is independent or not. Note that U. U. Umirbaev [386] showed that this problem for free associative algebras is algorithmically undecidable. Theorem 11.3.11 gives an effective algorithm to find the rank of a finitely generated subalgebra of A. These algorithms are based on the right weak algorithm. Another algorithm could be derived from Theorem 11.1.1. Indeed, using combinatorics on words, by elementary transformation we could transform the set H to a reduced set. The cardinality of this set is the rank of the subalgebra of A generated by H.

11.4 Stable Equivalence

An element u of a free algebra F is said to be primitive if it is an element of some set of free generators of the algebra F. A set of nonzero pairwise distinct elements of F is said to be a primitive system of elements if it is a subset of some set of free generators of F. The rank of $u \in F$ is the smallest number of generators from X on which an element $\varphi(u)$ depends, where φ runs through the automorphism group of F (in other words, $\operatorname{rank}(u)$ is the smallest rank of a free factor of F containing u). In the same way, the rank of a system of elements is defined.

In this section, we are interested in the following problems.

Problem 11.4.1. Let A be a free subalgebra of a free algebra F. Given two elements $u, v \in A$ such that there exists an automorphism φ of F with $\varphi(u) = v$, does there exist an automorphism ψ of A such that $\psi(u) = v$?

Problem 11.4.2. Let A be a free subalgebra of a free algebra F, u a primitive element of F, and $u \in A$. Does it imply that u is actually a primitive element of the free algebra A?

For free groups F of finite rank, the affirmative answer to Problem 11.4.1 with A a free factor of F and to Problem 11.4.2 follows from [227, Propositions 1.4.17 and 1.5.4]. V. Shpilrain and J.-T. Yu [365] solved Problem 11.4.2 for polynomial algebras in two and three variables with A being a free factor of F; see Proposition 6.0.4.

Problem 11.4.2 has a positive solution for the main types of Schreier varieties of algebras.

Let K be a field, $\operatorname{char} K \neq 2$, $X = \{x_1, \ldots, x_n\}$, and $F = F(X)$ the free algebra without the unity element on the set X of free generators of one of the following varieties of algebras over a field K: the variety of all algebras, the variety of Lie algebras, varieties of color Lie superalgebras, the variety of Lie p-algebras, varieties of color Lie p-superalgebras, and varieties of commutative and anticommutative algebras.

Proposition 11.4.3 ([265]). *Let $A = \{a_1, \dots, a_l\}$ be a primitive system of elements of F and B a finitely generated subalgebra of F such that $A \subset B$. Then A is a primitive system in B.*

Proof. Let H be a finite generating set of B, and $H' = H \cup A$. Using a finite number of elementary transformations of H', we will come to a free generating set of B. We may suppose that $A \subseteq X$. We may use only the following elementary transformations: if $h_1, \dots, h_s \in H'$ and the leading part h_1° of the element h_1 belongs to the subalgebra generated by the leading parts $h_2^\circ, \dots, h_s^\circ$, $h_1^\circ = \theta(h_2^\circ, \dots h_s^\circ)$, then we set $h_1' = h_1 - \theta(h_2, \dots h_s)$. It is clear that using these elementary transformations (with possible cancellation of zeros) we may come to a free generating set Y of B such that $A \subseteq Y$. Thus A is a primitive system of elements of B. ■

Now we consider Problem 11.4.1. At first we show that in general form this problem has a negative solution. We illustrate this for free Lie algebras. Let $B = L(X)$ be the free Lie algebra, where $X = \{x, y, z\}$, A the subalgebra of B generated by the elements $a = x + [y, z]$, $b = y$, $c = [x, y]$. The set $\{a, b, c\}$ is reduced (relative to the ordinary degree function). By Theorem 11.1.1, this set is an independent subset of A. Let φ be the automorphism of B given by $\varphi(x) = a$, $\varphi(y) = y$, $\varphi(z) = z$. Let $u = c$ and $v = [a, b]$. Then $\varphi(u) = v$. At the same time $u, v \in A$, u is a primitive element of A. For any automorphism ψ of A, the element $\psi(u)$ is a primitive element of A. Thus $\psi(u) \neq v = \varphi(u) = [a, b] \in [A, A]$. We solve Problem 11.4.1 in the affirmative supposing that A is a free factor of the free algebra $F(X)$.

Theorem 11.4.4 ([267]). *Let X and Y be nonempty sets, $X \cap Y = \varnothing$, $u_i, v_i \in F(X)$, $u_i \neq 0$, $v_i \neq 0$, $i = 1, \dots, m$. Suppose that there is an automorphism φ of the algebra $F(X \cup Y)$ such that $\varphi(u_i) = v_i$, $i = 1, \dots, m$. Then there is an automorphism ψ of $F(X)$ with $\psi(u_i) = v_i$, $i = 1, \dots, m$. In other words, if two finite systems of elements of the free algebra $F(X)$ are stably equivalent, then they are equivalent.*

Proof. Let $X = \{x_1, \dots, x_n\}$, $U = \{u_1, \dots, u_m\}$, and $\operatorname{rank}_{F(X)}(U) = l$. We may suppose that elements of U depend only on $x_1, \dots, x_l \in X$. On the contrary, suppose that the system of elements $\Phi = \{\varphi(x_1), \dots, \varphi(x_l)\}$ depends on a free generator $y \in Y$. Let $d = \max_{i=1,\dots,m} \deg(v_i)$. Consider the generalized degree function μ on $X \cup Y$ given by $\mu(x) = 1$ with $x \in X$, $\mu(z) = 1$ with $z \in Y$, $z \neq y$, and $\mu(y) = d + 1$.

Using a sequence of elementary transformations, we transform the set Φ to a μ-reduced set $\Phi' = \{\varphi'(x_1), \dots, \varphi'(x_l)\}$. Since φ is an automorphism, Φ' is a primitive system of elements of $F(X \cup Y)$. It is clear that Φ' depends on y. We may assume that the element $\varphi'(x_1)$ depends on y. The sequence of elementary transformations $\Phi \to \Phi'$ induces the sequence of elementary automorphisms θ of $F(x_1, \dots, x_l)$, namely $\varphi'(x_i) = \varphi(\theta(x_i))$, $i = 1, \dots, l$. Since $\operatorname{rank}_{F(X)}(U) = l$ and $v_i = \varphi(u_i)$, $i = 1, \dots, m$, at least one element

of $V = \{v_1, \ldots, v_m\}$ depends on $\varphi'(x_1)$. One may assume that v_1 depends on $\varphi'(x_1)$. Since $v_1 \in F(X)$, $\mu(v_1) = \deg(v_1)$. At the same time, Φ' is a μ-reduced set and $\mu(\varphi'(x_1)) \geq \mu(y) = d + 1$. By Theorem 11.1.1,

$$\deg(v_1) = \mu(v_1) \geq \mu(\varphi'(x_1)) \geq d + 1 > d = \max_{i=1,\ldots m} \{\deg(v_i)\},$$

and we have come to a contradiction. This contradiction shows that actually $\Phi \subset F(X)$.

Since φ is an automorphism, Φ is a primitive system of $F(X \cup Y)$. Since $\Phi \subset F(X)$, by Proposition 11.4.3 we get that Φ is a primitive system of $F(X)$. Let $\{\bar{x}_{l+1}, \ldots, \bar{x}_n\}$ be a complement of Φ with respect to a free generating set of $F(X)$. Now we consider the automorphism ψ of $F(X)$ given by $\psi(x_i) = \varphi(x_i)$, $i = 1, \ldots, l$, and $\psi(x_j) = \bar{x}_j$, $j = l + 1, \ldots, n$. It is clear that ψ is an automorphism of $F(X)$ and $\psi(u_i) = v_i$, $i = 1, \ldots, m$. ■

Theorem 11.4.5 ([267]). *Let X and Y be nonempty sets, $X \cap Y = \varnothing$, and U a finite set of nonzero elements of $F(X)$. Then*

$$\operatorname{rank}_{F(X)}(U) = \operatorname{rank}_{F(X \cup Y)}(U).$$

In other words, the rank of the system U is equal to its stable rank.

Proof. Using free differential calculus, matrix criteria for systems of elements of $F(X)$ to have a given rank are obtained in Section 12.4 of Chapter 12, Theorems 12.4.7–12.4.10 (free Lie algebras and superalgebras were considered over fields of characteristic zero). The statement of the theorem follows from these criteria. Here we give the proof without use of free differential calculus (and without restriction of the characteristic of the ground field for free Lie algebras and superalgebras).

Let $l = \operatorname{rank}_{F(X)}(U)$ and $k = \operatorname{rank}_{F(X \cup Y)}(U)$. It is clear that $k \leq l$. Suppose that $k < l$. Then there is an automorphism φ of $F(X \cup Y)$ such that the set $V = \varphi(U)$ depends only on free generators $x_1, \ldots, x_k \in X$. In particular, $V \subset F(X)$. By Theorem 11.4.4, there is an automorphism ψ of the algebra $F(X)$ such that $V = \psi(U)$. Hence $\operatorname{rank}_{F(X)}(V) = \operatorname{rank}_{F(X)}(U) = l > k$, and we have come to a contradiction (the set V depends only on $x_1, \ldots, x_k$). It completes the proof. ■

11.5 The Rank of an Endomorphism

In this section, we consider the following problem.

Problem 11.5.1. Let φ be an injective endomorphism of a free algebra F and $0 \neq u \in F$. Is it true that $\operatorname{rank}(\varphi(u)) \geq \operatorname{rank}(u)$?

In order to solve this problem, we define the rank of an endomorphism of a free algebra of Schreier variety of algebras and prove in Theorems

11.5.3 and 11.5.4 that an injective endomorphism of maximal rank does not change the rank of systems of elements with maximal rank.

Lemma 11.5.2. *Let U be a system of elements of a free algebra $F(X)$. Suppose that a system V is obtained from U by a finite sequence of elementary transformations. Then* $\operatorname{rank}(V) = \operatorname{rank}(U)$.

Proof. Suppose that $\operatorname{rank}(V) < \operatorname{rank}(U)$. Then there is an automorphism φ of $F(X)$ such that the system of elements $\varphi(V)$ depends only on $\operatorname{rank}(V)$ free generators from X. Since elementary transformations are invertible, the set U belongs to the subalgebra of $F(X)$ generated by V. Therefore the set $\varphi(U)$ belongs to the subalgebra of $F(X)$ generated by the set $\varphi(V)$, and

$$\operatorname{rank}(U) = \operatorname{rank}(\varphi(U)) \leq \operatorname{rank}(\varphi(V)) = \operatorname{rank}(V) < \operatorname{rank}(U).$$

This contradiction shows that $\operatorname{rank}(V) \geq \operatorname{rank}(U)$. Since there is a sequence of elementary transformations $V \to U$, we get $\operatorname{rank}(U) \geq \operatorname{rank}(V)$. Thus $\operatorname{rank}(V) = \operatorname{rank}(U)$. ■

Let φ be an endomorphism of $F(X)$, where $X = \{x_1, \ldots, x_n\}$. For the rank of φ ($\operatorname{rank}(\varphi)$), we take the rank of the system of elements $\varphi(X) = \{\varphi(x_1), \ldots, \varphi(x_n)\}$. This notion does not depend on the choice of free generators of the free algebra $F(X)$. Indeed, let $Y = \{y_1, \ldots, y_n\}$ be another set of free generators of $F(X)$. By Theorem 11.1.1, there is a sequence of elementary automorphisms $\psi\colon X \to Y$. This sequence induces the sequence of elementary transformations ψ' of the set $\varphi(X)$, $\psi'\colon Y = \varphi(X) \to \varphi(Y) = \{\varphi(y_1), \ldots, \varphi(y_n)\}$. By Lemma 11.5.2, $\operatorname{rank}(\varphi(Y)) = \operatorname{rank}(\varphi(X))$.

Let φ be an endomorphism of $F(X)$, $0 \neq u \in F(X)$. If u or φ is not of maximal rank, or φ is not injective, then in general there is no relation between $\operatorname{rank}(\varphi(u))$ and $\operatorname{rank}(u)$. We illustrate this for free Lie algebras.

Let $L(X)$ be the free Lie algebra, where $X = \{x, y\}$, φ the endomorphism of $L(X)$ given by $\varphi(x) = x$, $\varphi(y) = 0$, and $u = x + [x, y]$. Then $\varphi(u) = x$ and $\operatorname{rank}(\varphi(u)) = 1 < 2 = \operatorname{rank}(u) = |X|$. If ψ is the endomorphism of $L(X)$ given by $\psi(x) = u$, $\psi(y) = 0$, then $\psi(u) = u$, and $\operatorname{rank}(\psi(u)) = 2 = \operatorname{rank}(u)$. If $v = x$, then $\psi(v) = u$, and $\operatorname{rank}(\psi(v)) = 2 > \operatorname{rank}(v) = 1$.

If φ is an injective endomorphism of maximal rank, but $\operatorname{rank}(u) < n = |X|$, then we consider the following examples. Let $X = \{x, y, z, w\}$, and let φ be the endomorphism of the free Lie algebra $L(X)$ given by $\varphi(x) = x$, $\varphi(y) = [x, y]$, $\varphi(z) = [[x, y], y]$, $\varphi(w) = [z, w]$. Since the set $\{\varphi(x), \varphi(y), \varphi(z), \varphi(w)\}$ is reduced relative to the ordinary degree, φ is injective. Let $u_1 = [[x, y], z]$, $u_2 = [x, y]$, and $u_3 = [x, w]$. Then $\varphi(u_1) = [[x, [x, y]], [[x, y], y]]$, $\varphi(u_2) = [x, [x, y]]$, $\varphi(u_3) = [x, [z, w]]$, and

we get

$$\begin{aligned}\operatorname{rank}(\varphi(u_1)) &= 2 < 3 = \operatorname{rank}(u_1),\\ \operatorname{rank}(\varphi(u_2)) &= 2 = 2 = \operatorname{rank}(u_2),\\ \operatorname{rank}(\varphi(u_3)) &= 3 > 2 = \operatorname{rank}(u_3).\end{aligned}$$

In the case where φ is an injective endomorphism of $F(X)$, $0 \neq u \in F(X)$, both u and φ have maximal rank and we are able to prove that $\operatorname{rank}(\varphi(u)) = \operatorname{rank}(u)$.

Theorem 11.5.3 ([267]). *Let* $X = \{x_1, \ldots, x_n\}$, $0 \neq u \in F(X)$, *and* $\operatorname{rank}(u) = n$. *Let also* φ *be an injective endomorphism of* $F(X)$, $\operatorname{rank}(\varphi) = n$. *Then* $\operatorname{rank}(\varphi(u)) = \operatorname{rank}(u) = n$.

Proof. Suppose that $\operatorname{rank}(\varphi(u)) < n$. Then there is an automorphism ψ of $F(X)$ such that the element $\psi(\varphi(u))$ does not depend on x_n. It is clear that the endomorphism $\varphi' = \psi \circ \varphi$ is injective and $\operatorname{rank}(\varphi') = \operatorname{rank}(\varphi) = n$. Consider the generalized degree function μ given by

$$\mu(x_1) = \cdots = \mu(x_{n-1}) = 1, \quad \mu(x_n) = \deg(\varphi'(u)) + 1.$$

We transform the set $\varphi'(X) = \{\varphi'(x_1), \ldots, \varphi'(x_n)\}$ to a μ-reduced set $\varphi''(X)$ by a finite sequence of elementary transformations. Since φ is injective, the set $\varphi''(X)$ consists of n nonzero elements. It is clear that the set $\varphi''(X)$ depends on x_n, and the element $\varphi'(u)$ is a polynomial in free generators $\varphi''(X)$ $(F(\varphi''(X)) = F(\varphi'(X)))$. Since $\operatorname{rank}(u) = n$, the element $\varphi'(u)$ depends on every free generator from $\varphi''(X)$. Since the set $\varphi''(X)$ depends on x_n, by Theorem 11.1.1 we get

$$\deg(\varphi'(u)) = \mu(\varphi'(u)) \geq \mu(x_n) = \deg(\varphi'(u)) + 1.$$

This contradiction completes the proof. ■

The idea of the proof of Theorem 11.5.3 works also for systems of elements. Thus we have:

Theorem 11.5.4. *Let* $X = \{x_1, \ldots, x_n\}$. *Let also* $U = \{u_1, \ldots, u_m\}$ *be a system of nonzero elements of the free algebra* $F(X)$, $\operatorname{rank}(U) = n$, φ *an injective endomorphism of* $F(X)$, $\operatorname{rank}(U) = \operatorname{rank}(\varphi) = n$. *Then*

$$\operatorname{rank}(\{\varphi(u_1), \ldots, \varphi(u_m)\}) = \operatorname{rank}(U) = n.$$

In connection with Theorem 11.5.4, see Theorem 12.7.2 in Section 12.7 of Chapter 12 about inverse images of primitive systems of elements.

12

Rank Theorems and Primitive Elements

In this chapter, we consider automorphic orbits and combinatorial properties of primitive elements in free algebras of the main types of Schreier varieties of algebras. A system of elements of a free algebra F is called primitive if it is a subset of some set of free generators of F. The rank of a system of elements of a free algebra F is the minimal number of generators from X on which automorphic images of these elements can depend.

Let A be a finitely generated free algebra of the variety $\mathfrak{M}_0$ (the variety of all algebras), $\mathfrak{M}_1$ (the variety of all commutative algebras, $\operatorname{char} K \neq 2$), or $\mathfrak{M}_2$ (the variety of all anticommutative algebras).

In Sections 12.1 and 12.2, we consider basic properties of partial derivatives of elements of A. Some of these properties are based on differential separability of subalgebras of A and on the fact that the universal multiplicative enveloping algebra $U(A)$ is a free associative algebra that is a free ideal ring.

Section 12.3 is devoted to elimination of variables. Proposition 12.3.2 shows that if we have a dependence of derivatives of a homogeneous element, then there is an automorphism that eliminates a variable in the image of this element.

In Section 12.4, we obtain the rank theorems. Theorems 12.4.7 and 12.4.8 show that the rank of a system of elements is equal to the rank of the free module generated by the elements whose components are partial derivatives of elements of this system. Theorems 12.4.9 and 12.4.10 are the rank theorems for free Lie algebras and superalgebras.

In Section 12.5, we study primitive systems of elements and actions of endomorphisms on automorphic orbits of elements. Theorem 12.5.1 gives

a matrix characterization of primitive systems of elements: a system of elements of A is primitive if and only if the matrix of partial derivatives of elements of the system is left invertible over $U(A)$. In particular, an element of A is primitive if and only if its gradient is unimodular. Based on Theorems 12.4.7–12.5.1, we obtain in Theorem 12.5.2 algorithms to find the rank of a system of elements and to decide whether this system is primitive or not. Theorems 12.5.3–12.5.8 give matrix characterizations of primitive systems of elements in free Lie algebras and superalgebras. Using the Freiheitssatz, we obtain another characterization of primitive elements in Theorem 12.5.15: an element a of A is primitive if and only if the factor algebra of A by the ideal generated by a is a free algebra in the same variety of algebras.

In Section 12.6, we consider actions of endomorphisms on primitive elements. Theorem 12.6.2 shows that endomorphisms of A preserving primitivity of elements are automorphisms (Theorem 12.6.3 shows that this statement is true for free Lie algebras and superalgebras). Using this result, we obtain a more general statement in Section 13.3 of Chapter 13. Theorem 13.3.3 says that if an endomorphism of A preserves the automorphic orbit of a nonzero element, then it is an automorphism of A. In Theorems 12.6.6–12.6.8 and Problems 12.6.9 and 12.6.10, we consider images of nonzero linear combinations of free generators.

Section 12.7 deals with inverse images of primitive elements of free algebras of the main types of Schreier varieties of algebras under the action of endomorphisms. Theorems 12.7.1 and 12.7.2 show that inverse images of primitive systems of elements under the action of injective endomorphisms are primitive. In the general case, inverse images of primitive elements generate a retract (Theorem 12.7.3).

12.1 Basic Properties of Partial Derivatives

Let A be a finitely generated free algebra of the variety $\mathfrak{M}_0$ (the variety of all algebras), $\mathfrak{M}_1$ (the variety of all commutative algebras, $\operatorname{char} K \neq 2$), or $\mathfrak{M}_2$ (the variety of all anticommutative algebras).

Let H be a subalgebra of A. By J_H we denote the submodule of the module I_A generated by the elements $\{\mathcal{D}(h) \mid h \in H\}$. A variety $\mathfrak{M}$ has a property of differential separability for subalgebras if for any $a \in A$ we have $a \in H$ if and only if $\mathcal{D}(a) \in J_H$. The varieties $\mathfrak{M}_0$ and $\mathfrak{M}_2$ have the property of differential separability for subalgebras. If $\operatorname{char} K \neq 2$, then the variety $\mathfrak{M}_1$ also has this property. For the details, we refer to [388].

In all of what follows, by $\mathfrak{M}$ we will denote one of the varieties $\mathfrak{M}_0$, $\mathfrak{M}_1$ ($\operatorname{char} K \neq 2$), and $\mathfrak{M}_2$. Also, we use the notations W_i for the linear basis of the algebra A and S_i for the set of free generators of the algebra $U(A)$.

The structure of a $U(A)$-module on A is given by $a \cdot r_w = a \cdot w$, $a \cdot l_w = w \cdot a$ $(a, w \in A)$.

Let H be the subalgebra of A generated by $x_1, \ldots, x_{n-1}$, $U(H)$ the subalgebra with the unit element of $U(A)$ generated by $\{r_u, l_u \mid u \in H\}$, and $S_H = S \cap U(H)$. In the general case, if H is a subalgebra of A, then $U(H)$ is not necessarily a subalgebra of $U(A)$. But for Schreier varieties of algebras, $U(H)$ is a subalgebra of $U(A)$. Let V_H be the left ideal of $U(A)$ generated by the elements r_u and l_u, where u runs through all monomials in $x_1, \ldots, x_{n-1}$ of the degree not less than 1.

Lemma 12.1.1. *For any $a \in A$ and $u \in U(H)$*

$$\frac{\partial}{\partial x_n}(a \cdot u) = \frac{\partial}{\partial x_n}(a) \cdot u.$$

Proof. One may assume that u is a monomial in S_H. Let $u = u_1 \cdot s$, where either $s = r_h$ or $s = l_h$, $h \in H$. Since $h \in H$, $\frac{\partial h}{\partial x_n} = 0$. Hence

$$\frac{\partial}{\partial x_n}((a \cdot u_1) \cdot r_h) = \frac{\partial a u_1}{\partial x_n} \cdot r_h + \frac{\partial h}{\partial x_n} \cdot l_{au_1} = \frac{\partial a u_1}{\partial x_n} \cdot r_h,$$
$$\frac{\partial}{\partial x_n}((a \cdot u_1) \cdot l_h) = \frac{\partial h}{\partial x_n} \cdot r_{au_1} + \frac{\partial a u_1}{\partial x_n} \cdot l_h = \frac{\partial a u_1}{\partial x_n} \cdot l_h;$$

that is, $\frac{\partial a \cdot u}{\partial x_n} = \frac{\partial a u_1}{\partial x_n} s$. Applying the induction on the S-degree, we complete the proof. ■

Lemma 12.1.2. *If $a \in A$ and $\frac{\partial a}{\partial x_n} = 0$, then $a \in H$.*

Proof. If $\frac{\partial a}{\partial x_n} = 0$, then

$$\mathcal{D}(a) = y_1 \frac{\partial a}{\partial x_1} + \cdots + y_{n-1} \frac{\partial a}{\partial x_{n-1}} \in J_H.$$

Since the variety $\mathfrak{M}$ has the property of differential separability for subalgebras, it follows that $a \in H$. ■

Lemma 12.1.3. *If $a \in A$ and $\frac{\partial a}{\partial x_n} \in V_H$, then the element a has a presentation $a = \sum \alpha_i u_i v_i + a'$, where $\alpha_i \in K$, $u_i, v_i \in W$, $a' \in H$, and for every i either $u_i \in H$ or $v_i \in H$.*

Proof. Since algebras A and $U(A)$ and the ideal V_H are homogeneous with respect to any $x_i \in X$, it is enough to prove the statement for a multihomogeneous element a. If a does not depend on x_n, then $\frac{\partial a}{\partial x_n} = 0$. If $a = \alpha x_n$ with $\alpha \neq 0$, then $\frac{\partial a}{\partial x_n} = \alpha \notin V_H$. Therefore we suppose that a is a multihomogeneous element of degree not less than 2, and a depends on x_n. Then a has the unique presentation in the form $a = \sum \alpha_i u_i v_i$, where $u_i, v_i \in W$, $\alpha_i \in K$.

If $\mathfrak{M} = \mathfrak{M}_0$, then

$$a = f_1 w_1 + f_2 w_2 + \ldots f_k w_k, \tag{12.1}$$

where f_i are linear combinations of words of W_0, $w_i \in W_0$, $w_1 > \cdots > w_k$. Then

$$\frac{\partial a}{\partial x_n} = \sum_{i=1}^{k} \frac{\partial f_i}{\partial x_n} \cdot r_{w_i} + \sum_{i=1}^{k} \frac{\partial w_i}{\partial x_n} l_{f_i}.$$

Since elements of $S_H = S \cap V_H$ are left independent over $U(A)$, it follows from $\frac{\partial a}{\partial x_n} \in V_H$ that $\frac{\partial f_i}{\partial x_n} r_{w_i} \in V_H$. Hence $w_i \in H$ or $\frac{\partial f_i}{\partial x_n} = 0$. By Lemma 12.1.2, we get either $f_i \in H$ or $w_i \in H$.

If $\mathfrak{M} = \mathfrak{M}_1$, then the element a has a presentation in the form (12.1), where f_i are linear combinations of monomials of W_1 less than or equal to w_i. Let $f_i = \alpha_i w_i + g_i$, $1 \leq i \leq k$, where g_i are linear combinations of monomials less than w_i. Then

$$\frac{\partial a}{\partial x_n} = \sum_{i=1}^{k} \left(2\alpha_i \frac{\partial w_i}{\partial x_n} + \frac{\partial g_i}{\partial x_n} \right) r_{w_i} + \sum_{i=1}^{k} \frac{\partial w_i}{\partial x_n} r_{g_i}.$$

Since $w_1 > w_2 > \cdots > w_n$, r_{g_i} has no terms of the form αr_{w_1}, $\alpha \in K$. Hence, if $\frac{\partial a}{\partial x_n} \in V_H$, then

$$\left(2\alpha_1 \frac{\partial w_1}{\partial x_n} + \frac{\partial g_1}{\partial x_n} \right) r_{w_1} \in V_H.$$

It follows that either $w_1 \in H$ or $\frac{\partial (2\alpha_1 w_1 + g_1)}{\partial x_n} = 0$; that is, either $w_1 \in H$ or $2\alpha_1 w_1 + g_1 \in H$. Denote $b = a - (2\alpha_1 w_1 + g_1) w_1$. We have $b = -\alpha_1 w_1 w_1 + \sum_{i=2}^{k} f_i w_i$, $\frac{\partial b}{\partial x_n} \in V_H$, and

$$\frac{\partial b}{\partial x_n} = -2\alpha_1 \frac{\partial w_1}{\partial x_n} r_{w_1} + \sum_{i=2}^{k} \left(\frac{\partial f_i}{\partial x_n} r_{w_i} + \frac{\partial w_i}{\partial x_n} r_{f_i} \right) \in V_H.$$

Therefore $2\alpha_1 \frac{\partial w_1}{\partial x_n} r_{w_1} \in V_H$. We consider the variety $\mathfrak{M}_1$ over a field K of characteristic different from 2. Thus $\alpha_1 = 0$, $\frac{\partial w_1}{\partial x_n} = 0$, or $w_1 \in H$. The condition $\frac{\partial w_1}{\partial x_n} = 0$ is equivalent to $w_1 \in H$, so we get $\alpha_1 = 0$ or $w_1 \in H$, and it is enough to prove the statement of the lemma for the element $b + \alpha_1 w_1 w_1 = \sum_{i=2}^{k} f_i w_i$. The induction on k for the presentation (12.1) completes the proof.

If $\mathfrak{M} = \mathfrak{M}_2$, then the element a has the presentation (12.1), where f_i are linear combinations of monomials less than w_i. As in the proof for $\mathfrak{M}_1$, it follows from $\frac{\partial a}{\partial x_n} \in V_H$ that $\frac{\partial f}{\partial x_n} r_{w_1} \in V_H$; that is, $w_1 \in H$ or $f_1 \in H$. Considering the element $b = a - f_1 w_1$ and using the induction on the length of the presentation (12.1), we complete the proof of the lemma. ■

12.2 Homogeneous Admissible Elements

Let $\mathbb{Z}_+ = \{k \in \mathbb{Z} \mid k \geq 0\}$, $\mathbb{Q}_+ = \{\alpha \in \mathbb{Q} \mid \alpha \geq 0\}$. We say that a monomial $w \in W$ has the multidegree $m(w) = (k_1, \ldots, k_n) \in \mathbb{Z}_+^n$ if for each $i = 1, \ldots, n$ the generator x_i occurs in w exactly k_i times. A linear mapping $\mu\colon \mathbb{Z}_+^n \to \mathbb{Q}_+$ is a functional if $\mu(s) \neq 0$ for all nonzero $s \in \mathbb{Z}_+^n$. For $w \in W$, we introduce the μ-degree by $\mu(w) = \mu(m(w))$. An element $a = \sum_{i=1}^k \alpha_i w_i$, $w_i \in W$ is said to be μ-homogeneous (m-homogeneous) if $\mu(w_1) = \cdots = \mu(w_k)$ ($m(w_1) = \cdots = m(w_k)$, respectively). For $w \in W$ we set $m(r_w) = m(l_w) = m(w)$ and $\mu(r_w) = \mu(l_w) = \mu(w)$. This gives us a possibility to consider μ-homogeneous and m-homogeneous elements of the universal multiplicative enveloping algebra $U(A)$. The algebra $U(A)$ is the free associative algebra with the set S of free generators. Therefore elements of $U(A)$ have the S-degree.

We say that a set $\{u_1, \ldots, u_k\}$ of μ-homogeneous elements of $U(H)$ is admissible if it follows from the equation

$$\frac{\partial a}{\partial x_n} = \sum_{i=1}^{k} m_i u_i, \tag{12.2}$$

where $a \in A$, $m_1, \ldots, m_k \in U(A)$, that there exist $a_1, \ldots, a_k \in A$ such that

$$\frac{\partial a}{\partial x_n} = \sum_{i=1}^{k} \frac{\partial a_i}{\partial x_n} u_i.$$

Lemma 12.2.1.

(i) *A set with zero elements is an admissible set.*

If $\{u_1, \ldots, u_k\}$ *is an admissible set, then:*

(ii) *The set* $\{u_1, \ldots, u_k, 0\}$ *is admissible.*

(iii) *The set* $\{u_{\sigma(1)}, \ldots, u_{\sigma(k)}\}$ *is admissible for any element* σ *of the symmetric group* S_k.

(iv) *If* $0 \neq \alpha \in K$, *then the set* $\{u_1, \ldots, u_{k-1}, \alpha u_k\}$ *is admissible.*

(v) *If* $u \in U(H)$ *and the element* $u_k + uu_{k-1}$ *is* μ*-homogeneous, then* $\{u_1, \ldots, u_{k-1}, u_k + uu_{k-1}\}$ *is an admissible set.*

Proof. The statements of points (i)–(iv) are obvious. To prove (v), suppose that

$$\frac{\partial a}{\partial x_n} = \sum_{i=1}^{k-1} m_i u_i + m_k(u_k + uu_{k-1}) = \sum_{i=1}^{k-2} m_i u_i + (m_{k-1} + m_k u)u_{k-1} + m_k u_k.$$

By the conditions of the lemma, there are $a_1, a_2, \ldots, a_k \in A$ such that

$$\frac{\partial a}{\partial x_n} = \sum_{i=1}^{k} \frac{\partial a_i}{\partial x_n} u_i.$$

Therefore

$$\begin{aligned}\frac{\partial a}{\partial x_n} &= \sum_{i=1}^{k} \frac{\partial a_i}{\partial x_n} u_i + \frac{\partial a_k}{\partial x_n} u u_{k-1} - \frac{\partial a_k}{\partial x_n} u u_{k-1} \\ &= \sum_{i=1}^{k-2} \frac{\partial a_i}{\partial x_n} u_i + \left(\frac{\partial a_{k-1}}{\partial x_n} - \frac{\partial a_k}{\partial x_n} u \right) u_{k-1} + \frac{\partial a_k}{\partial x_n} (u_k + u u_{k-1}) \\ &= \sum_{i=1}^{k-2} \frac{\partial a_i}{\partial x_n} u_i + \frac{\partial}{\partial x_n} (a_{k-1} - a_k u) u_{k-1} + \frac{\partial a_k}{\partial x_n} (u_k + u u_{k-1}).\end{aligned}$$

Thus the set $\{u_1, \ldots, u_{k-1}, u_k + u u_{k-1}\}$ is admissible. ■

Lemma 12.2.2. *Suppose that elements $a \in A$, $m_1, \ldots, m_k \in U(A)$, and μ-homogeneous elements $u_1, \ldots, u_k \in U(H)$ satisfy the equation* (12.2)*, and $\mu(u_1) \leq \mu(u_i)$ with $i \geq 2$. If there is an S-monomial u having a nonzero coefficient in the presentation of u_1 such that elements $u_2, \ldots, u_k$ have no monomials ending on u, then $m_1 \in \frac{\partial}{\partial x_n}(A)$.*

Proof. We use the induction on the S-degree of the monomial u. If $u = 1$, then $u_1 = \alpha u$, $0 \neq \alpha \in K$, and $u_2 = \cdots = u_k = 0$, and

$$m_1 = \frac{1}{\alpha} \sum_{i=1}^{k} m_i a_i = \frac{1}{\alpha} \frac{\partial a}{\partial x_n} \in \frac{\partial}{\partial x_n}(A).$$

It is clear that $u \in U(H)$. Let $u = u_0 s$, where $s \in S$. Consider $w \in H$ such that either $s = r_w$ or $s = l_w$. Since $0 < \mu(u_1) \leq \mu(u_i)$, $i \geq 2$, it follows from (12.2) that $\frac{\partial a}{\partial x_n} \in V_H$. By Lemma 12.1.3, $a = \sum_i \alpha_i w_i v_i$, where for any i either $w_i \in H$ or $v_i \in H$. We write down the element a in the form

$$a = \alpha w \cdot w + w \cdot f + g \cdot w + \sum \beta_j w_j v_j,$$

where f and g are linear combinations of basic monomials different from w and $w_j, v_j \neq w$, and for any i either $w_j \in H$ or $v_j \in H$. We get

$$\frac{\partial a}{\partial x_n} = \frac{\partial f}{\partial x_n} l_w + \frac{\partial g}{\partial x_n} r_w + \sum_j \beta_j \left(\frac{\partial w_j}{\partial x_n} r_{v_j} + \frac{\partial v_j}{\partial x_n} l_{w_j} \right).$$

The elements u_i have the unique presentation in the form $u_i = u_i' s + u_i''$, $1 \leq i \leq k$, where elements u_i'' have no monomials ending on s.

Let $s = r_w$. Since $U(A)$ is the free algebra on S, comparing in (12.2) monomials ending on s, we obtain $\frac{\partial g}{\partial x_n} = \sum_{i=1}^{k} m_i u_i'$. It is easy to see that u_0 has a nonzero coefficient in u_1' and elements $u_2', \ldots, u_k'$ have no S-monomials ending on u_0. Hence we have proved the statement for u_0. Since the S-degree of u_0 is less than the S-degree of u, by induction we get $m_1 \in \frac{\partial}{\partial x_n}(A)$. ■

Lemma 12.2.3. *Any subset $\{u_1, u_2, \ldots, u_k\}$ of μ-homogeneous elements of $U(H)$ is admissible.*

Proof. We apply the induction on k. Let $k = 1$. If $u_1 = 0$, then our statement follows from Lemma 12.2.1. Suppose that $u_1 \neq 0$, and for some $a \in A$ and $m_1 \in U(A)$ we have $\frac{\partial a}{\partial x_n} = m_1 u_1$. Consider any S-monomial u that has a nonzero coefficient in u_1. By Lemma 12.2.2, $m_1 \in \frac{\partial}{\partial x_n}(A)$.

Let $k > 1$. By Lemma 12.2.1, we may assume that $\mu(u_1) \leq \mu(u_i)$ with $i \geq 2$. Consider an S-monomial u entering in u_1 with a nonzero coefficient α. One may suppose that $\alpha = 1$. For the elements u_i, $i \geq 2$, we have the presentation in the form $u_i = u_i' u + u_i''$, where u_i'' have no monomials ending on u. By Lemma 12.2.1, the set $\{u_1, \ldots, u_k\}$ is admissible if and only if the set $\{u_1, u_2 - u_2' u_1, \ldots, u_k - u_k' u_1\}$ is admissible. Since the element u_1 is μ-homogeneous, the element $u_1 - u$ has no monomials ending on u. Therefore, for $i \geq 2$, the element

$$u_i - u_i' u_1 = u_i' u + u_i'' - u_i' u_1 = u_i'(u - u_1) + u_i''$$

has no monomials ending on u. Hence, we may suppose that elements $u_2, \ldots, u_k$ have no monomials ending on u. By Lemma 12.2.2, $m_1 = \frac{\partial a_1}{\partial x_n}$ for some $a_1 \in A$. Thus

$$\frac{\partial a}{\partial x_n} = \frac{\partial a_1}{\partial x_n} u_1 + \sum_{i=2}^{k} m_i u_i.$$

Applying Lemma 12.1.1, we get

$$\frac{\partial a}{\partial x_n} - \frac{\partial a_1}{\partial x_n} u_1 = \frac{\partial}{\partial x_n}(a - a_1 u_1) = \sum_{i=2}^{k} m_i u_i.$$

By the induction hypothesis, there are $a_2, \ldots, a_k \in A$ such that

$$\frac{\partial a}{\partial x_n} - \frac{\partial a_1}{\partial x_n} u_1 = \sum_{i=2}^{k} \frac{\partial a_i}{\partial x_n} u_i;$$

that is, the set $\{u_1, \ldots, u_k\}$ is admissible. ■

Lemma 12.2.4. *Suppose that elements $u_1, u_2, \ldots, u_k$ of $U(H)$ are left independent over $U(A)$. Then, if for some $a \in A$, $m_1, \ldots, m_k \in U(A)$ the equation* (12.2) *is fulfilled, then $m_i \in \frac{\partial}{\partial x_n}(A)$, $1 \leq i \leq k$.*

Proof. By Lemma 12.2.3, there are $a_1, \ldots, a_k$ of A such that $\frac{\partial u}{\partial x_n} = \sum_{i=1}^{k} \frac{\partial a_i}{\partial x_n} u_i$. Then $\sum_{i=1}^{k} (m_i - \frac{\partial a_i}{\partial x_n}) u_i = 0$. Since elements $u_1, \ldots, u_k$ are left independent over $U(A)$, $m_i = \frac{\partial a_i}{\partial x_n} \in \frac{\partial}{\partial x_n}(A)$, $1 \leq i \leq k$. ■

12.3 Elimination of Variables

An endomorphism φ of the algebra A is said to be μ-homogeneous if $\varphi(x_i)$, $i = 1, \ldots, n$ are μ-homogeneous elements, and $\mu(\varphi(x_i)) = \mu(x_i)$, $x_i \in X$.

The matrix

$$J(\varphi) = (\partial(\varphi(x_1)), \partial(\varphi(x_2)), \ldots, \partial(\varphi(x_n))) \in M_n(U(A))$$

is the Jacobian matrix of the endomorphism φ. An endomorphism φ is an automorphism of A if and only if the matrix $J(\varphi)$ is invertible over $U(A)$ ([388, 406]). For any $k \leq n$, we set

$$J_k(\varphi) = \begin{pmatrix} \frac{\partial\varphi(x_1)}{\partial x_1} & \cdots & \frac{\partial\varphi(x_k)}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial\varphi(x_1)}{\partial x_k} & \cdots & \frac{\partial\varphi(x_k)}{\partial x_k} \end{pmatrix}.$$

It is clear that $J_n(\varphi) = J(\varphi)$.

Lemma 12.3.1. *Let k be an integer, $1 \leq k \leq n$, and let φ be a μ-homogeneous automorphism of A such that $\varphi(x_i) = x_i$ for all $i > k$. Then the matrix $J_k(\varphi)$ is invertible. If $B = (b_{ij}) = (J_k(\varphi))^{-1}$, then all elements b_{ij} are μ-homogeneous and $\mu(b_{ij}) = \mu(x_j) - \mu(x_i)$ (here, if $\mu(x_j) - \mu(x_i) < 0$, then $b_{ij} = 0$).*

The proof of this lemma is straightforward.

The main result of this section is the following proposition:

Proposition 12.3.2 ([259]). *Let a be a μ-homogeneous element of A and $k < n$. Suppose that there are μ-homogeneous elements $m_1, m_2, \ldots, m_k$ of $U(A)$ such that $\mu(m_i) = \mu(x_i) - \mu(x_n)$ for all $i \leq k$ and*

$$\frac{\partial a}{\partial x_n} = \sum_{i=1}^{k} m_i \frac{\partial a}{\partial x_i}. \tag{12.3}$$

Then there is a μ-homogeneous automorphism φ of A such that $\varphi(x_i) = x_i$ for all $i > k$ and $\varphi(a) \in H$, where H is the subalgebra of A generated by $x_1, \ldots, x_{n-1}$.

In order to prove Proposition 12.3.2, at first we prove the following lemmas.

Lemma 12.3.3. *Suppose that a positive integer k and an element a of A satisfy the conditions of Proposition 12.3.2. If φ is a μ-homogeneous automorphism of A such that $\varphi(x_i) = x_i$ for all $i > k$, then k and $\varphi(a)$ also satisfy the conditions of Proposition 12.3.2.*

Proof. Since

$$\frac{\partial(\varphi(a))}{\partial x_j} = \sum_{i=1}^{n} \frac{\partial(\varphi(x_i))}{\partial x_j} \varphi\left(\frac{\partial a}{\partial x_i}\right)$$

and $\varphi(x_s) = x_s$ with $s > k$,

$$\frac{\partial(\varphi(a))}{\partial x_j} = \sum_{i=1}^{k} \frac{\partial \varphi(x_i)}{\partial x_j} \varphi\left(\frac{\partial a}{\partial x_i}\right), \quad 1 \le j \le k,$$

$$\frac{\partial(\varphi(a))}{\partial x_n} = \varphi\left(\frac{\partial a}{\partial x_n}\right) + \sum_{i=1}^{k} \frac{\partial \varphi(x_i)}{\partial x_n} \varphi\left(\frac{\partial a}{\partial x_i}\right).$$

By (12.3), for any $m'_1, \ldots, m'_k \in U(A)$, we have

$$\begin{aligned}
\frac{\partial(\varphi(a))}{\partial x_n} - \sum_{j=1}^{k} m'_j \frac{\partial(\varphi(a))}{\partial x_j} &= \varphi\left(\frac{\partial a}{\partial x_n}\right) \\
&+ \sum_{i=1}^{k} \frac{\partial(\varphi(x_i))}{\partial x_n} \varphi\left(\frac{\partial a}{\partial x_i}\right) - \sum_{j=1}^{k} m'_j \left(\sum_{i=1}^{k} \frac{\partial(\varphi(x_i))}{\partial x_j} \varphi\left(\frac{\partial a}{\partial x_i}\right)\right) \\
&= \sum_{i=1}^{k} \varphi(m_i) \varphi\left(\frac{\partial a}{\partial x_i}\right) + \sum_{i=1}^{k} \frac{\partial(\varphi(x_i))}{\partial x_n} \varphi\left(\frac{\partial a}{\partial x_i}\right) \\
&- \sum_{i=1}^{k} \left(\sum_{j=1}^{k} m'_j \frac{\partial(\varphi(x_i))}{\partial x_j} \right) \varphi\left(\frac{\partial a}{\partial x_i}\right) \\
&= \sum_{i=1}^{k} \left(\varphi(m_i) + \frac{\partial(\varphi(x_i))}{\partial x_n} - \sum_{j=1}^{k} m'_j \frac{\partial(\varphi(x_i))}{\partial x_j} \right) \varphi\left(\frac{\partial a}{\partial x_i}\right).
\end{aligned}$$

Consider the system of equations (with unknowns $m'_1, \ldots, m'_k$)

$$\varphi(m_i) + \frac{\partial(\varphi(x_i))}{\partial x_n} = \sum_{j=1}^{k} m'_j \frac{\partial(\varphi(x_i))}{\partial x_j}, \quad 1 \le i \le k.$$

We write down this system in the matrix form $P = MJ_k(\varphi)$, where

$$\begin{aligned}
P &= \left(\varphi(m_1) + \frac{\partial(\varphi(x_i))}{\partial x_n}, \ldots, \varphi(m_k) + \frac{\partial(\varphi(x_k))}{\partial x_n} \right), \\
M &= (m'_1, m'_2, \ldots, m'_k).
\end{aligned}$$

By Lemma 12.3.1, this system has the unique solution

$$m'_j = \sum_{i=1}^{k} \left(\varphi(m_i) + \frac{\partial(\varphi(x_i))}{\partial x_n} \right) b_{ij}, \quad 1 \le j \le k,$$

where $B = (J_k(\varphi))^{-1} = (b_{ij})$. Remark that

$$\begin{aligned}
\mu(m'_j) = \mu(\varphi(m_i) \cdot b_{ij}) &= \mu\left(\frac{\partial(\varphi(x_i))}{\partial x_n} \cdot b_{ij} \right) \\
&= \mu(x_i) - \mu(x_n) + \mu(x_j) - \mu(x_i) = \mu(x_j) - \mu(x_n).
\end{aligned}$$

It follows from $\frac{\partial(\varphi(a))}{\partial x_n} = \sum_{j=1}^{k} m'_j \frac{\partial(\varphi(a))}{\partial x_j}$ that k and $\varphi(a)$ satisfy the conditions of Proposition 12.3.2. ■

Consider the following decompositions of algebras A and $U(A)$:

$$A = A_0 \oplus A_1 \oplus \cdots \oplus A_k \oplus \ldots,$$
$$U(A) = U_0 \oplus U_1 \oplus \cdots \oplus U_k \oplus \ldots,$$

where A_i and U_i are subspaces of all homogeneous elements with respect to x_n with the x_n-degree equal to i, $A_0 = H$, $U_0 = U(H)$. For an element f of A (of $U(A)$, respectively), by $f^{(k)}$ we denote its component of A_k (of U_k, respectively).

Lemma 12.3.4. *Suppose that a positive integer k and an element a of A satisfy the conditions of Proposition 12.3.2, and there is a positive integer s, $1 \leq s \leq k$, such that the elements $\frac{\partial}{\partial x_1}(a^{(0)}), \ldots, \frac{\partial}{\partial x_s}(a^{(0)})$ are left independent and $\frac{\partial}{\partial x_{s+1}}(a^{(0)}) = \cdots = \frac{\partial}{\partial x_k}(a^{(0)}) = 0$. Then, for any $r > 0$, the following conditions are equivalent:*

(i) $a^{(1)} = a^{(2)} = \cdots = a^{(r)} = 0$;

(ii) $m_i^{(j)} = 0$ *for all* $i = 1, 2, \ldots, s$ *and* $j = 0, 1, \ldots, r-1$.

Proof. It follows from (12.3) that

$$\frac{\partial}{\partial x_n}(a^{(j+1)}) = \left(\frac{\partial a}{\partial x_n}\right)^{(j)} = \sum_{i=1}^{k} \left(m_i \frac{\partial a}{\partial x_i}\right)^{(j)}$$
$$= \sum_{i=1}^{k} \sum_{l=0}^{j} m_i^{(l)} \left(\frac{\partial a}{\partial x_i}\right)^{(j-l)} = \sum_{i=1}^{k} \sum_{l=0}^{j} m_i^{(l)} \frac{\partial}{\partial x_i}(a^{(j-l)}) \quad (12.4)$$

for all $j = 0, 1, \ldots, r-1$.

If (i) is fulfilled, then we rewrite (12.4) in the form

$$\sum_{i=1}^{k} m_i^{(j)} \frac{\partial}{\partial x_i}(a^{(0)}) = \sum_{i=1}^{s} m_i^{(j)} \frac{\partial}{\partial x_i}(a^{(0)}) = 0.$$

Bearing in mind that elements $\frac{\partial}{\partial x_i}(a^{(0)})$, $1 \leq i \leq s$, are left independent, we get (ii).

If (ii) is fulfilled, then we write down (12.4) in the form

$$\frac{\partial}{\partial x_n}(a^{(j+1)}) = \sum_{i=s+1}^{k} \sum_{l=0}^{j-1} m_i^{(l)} \frac{\partial}{\partial x_i}(a^{(j-l)}).$$

If $j = 0$, then $\frac{\partial}{\partial x_n}(a^{(1)}) = 0$. By Lemma 12.1.2, $a^{(1)} \in H = A_0$; that is, $a^{(1)} = 0$. Suppose that for some t, $t < r$, we have $a^{(1)} = a^{(2)} = \cdots =$

$a^{(t)} = 0$. Then, setting $j = t$ in the previous equality, we get

$$\frac{\partial}{\partial x_n}(a^{(t+1)}) = \sum_{i=s+1}^{k} \sum_{l=0}^{t-1} m_i^{(l)} \frac{\partial}{\partial x_i}(a^{(t-l)}) = 0.$$

Hence $a^{(t+1)} = 0$, and the induction on t completes the proof. ■

Lemma 12.3.5. *Suppose that all conditions of Lemma 12.3.4 are fulfilled. If* $a^{(1)} = a^{(2)} = \cdots = a^{(r)} = 0$ *for some* $r \geq 0$, *then there is a* μ*-homogeneous automorphism* φ *of* A *such that*

$$\varphi(x_i) = x_i \quad \text{with} \quad x > k, \quad (\varphi(a))^{(0)} = a^{(0)},$$
$$(\varphi(a))^{(1)} = (\varphi(a))^{(2)} = \cdots = (\varphi(a))^{(r)} = (\varphi(a))^{(r+1)} = 0.$$

Proof. It follows from (12.3) and (12.4) that

$$\frac{\partial}{\partial x_n}(a^{(r+1)}) = \sum_{i=1}^{k} \sum_{l=0}^{r} m_i^{(l)} \frac{\partial}{\partial x_i}(a^{(r-l)})$$
$$= \sum_{i=1}^{k} m_i^{(r)} \frac{\partial}{\partial x_i}(a^{(0)}) = \sum_{i=1}^{s} m_i^{(r)} \frac{\partial}{\partial x_i}(a^{(0)}).$$

Since elements $\frac{\partial}{\partial x_1}(a^{(0)}), \ldots, \frac{\partial}{\partial x_s}(a^{(0)})$ of $U(H)$ are left independent and μ-homogeneous, by Lemma 12.2.3 there are elements g_i of A such that $m_i^{(r)} = \frac{\partial g_i}{\partial x_n}$, $1 \leq i \leq s$. One may assume that the elements g_i are μ-homogeneous and $g_i \in A_{r+1}$, $1 \leq i \leq s$. Then

$$\mu(g_i) = \mu(m_i^{(r)}) + \mu(x_n) = \mu(m_i) + \mu(x_n) = \mu(x_i) - \mu(x_n) + \mu(x_n) = \mu(x_i).$$

Consider the homogeneous endomorphism φ of A given by

$$\varphi(x_i) = \begin{cases} x_i - g_i, & i \leq s; \\ x_i, & i > s. \end{cases}$$

Without loss of generality, we may assume that $\mu(x_1) \geq \mu(x_2) \geq \cdots \geq \mu(x_s)$. Since for $j \leq i \leq s$

$$\mu(m_i) = \mu(x_i) - \mu(x_n) < \mu(x_i) \leq \mu(x_j),$$

the element m_i does not depend on x_j. It follows from $m_i^{(r)} = \frac{\partial g_i}{\partial x_n}$ and $g_i \in A_{r+1}$ that g_i does not depend on x_j. Since $g_i \in A_{r+1}$ and $r + 1 > 0$,

$$\varphi(a) - a = -g_1 \frac{\partial a}{\partial x_1} - g_2 \frac{\partial a}{\partial x_2} - \cdots - g_s \frac{\partial a}{\partial x_s} + b,$$

where $b \in A_{2r+2} \oplus A_{2r+3} \oplus \ldots$. Moreover,

$$(\varphi(a))^{(l)} = a^{(l)}, \quad 0 \leq l \leq r,$$
$$(\varphi(a))^{(r+1)} - a^{(r+1)} = -\sum_{i=1}^{s} g_i \frac{\partial}{\partial x_i}(a^{(0)}).$$

Therefore

$$(\varphi(a))^{(r+1)} = a^{(r+1)} - \sum_{i=1}^{s} g_i \frac{\partial}{\partial x_i}(a^{(0)}).$$

Since $\frac{\partial}{\partial x_i}(a^{(0)}) \in U(H)$,

$$\frac{\partial}{\partial x_n}((\varphi(a))^{(r+1)}) = \frac{\partial}{\partial x_n}(a^{(r+1)}) - \sum_{i=1}^{s} \frac{\partial g_i}{\partial x_n}\frac{\partial}{\partial x_i}(a^{(0)})$$
$$= \frac{\partial}{\partial x_n}(a^{(r+1)}) - \sum_{i=1}^{s} m_i^{(r)} \frac{\partial}{\partial x_i}(a^{(0)}) = 0.$$

■

Lemma 12.3.6. *Suppose that all conditions of Lemma 12.3.4 are fulfilled. Then there is a μ-homogeneous automorphism φ of A such that $\varphi(a) \in H$ and $\varphi(x_i) = x_i$ with $i > k$.*

Proof. Using the induction on r (with the base $r = 0$) and Lemmas 12.3.5 and 12.3.3, for any r we find an automorphism φ_r with $\varphi(x_i) = x_i$ for $i > k$, $(\varphi_r(a))^{(0)} = a^{(0)}$, $(\varphi_r(a))^{(1)} = \cdots = (\varphi_r(a))^{(r)} = 0$. Take r such that $r + 1 > \frac{\mu(a)}{\mu(x_n)}$. If for some $s > r$ we have $(\varphi_r(a))^{(s)} \neq 0$, then

$$\mu(x_n) \cdot s \leq \mu(\varphi_r(a)) = \mu(a);$$

thus $r + 1 \leq s \leq \frac{\mu(a)}{\mu(x_n)}$. This contradiction shows that φ_r is a desirable automorphism. ■

Proof of Proposition 12.3.2. We use the induction on k. If $k = 0$, then $\frac{\partial a}{\partial x_n} = 0$; that is, $a \in H$, and for φ we may take the identical automorphism of A. Suppose that $k > 0$ and the statement is proved for all $k' < k$. We denote $b = a^{(0)}$. If the elements $\frac{\partial b}{\partial x_1}, \frac{\partial b}{\partial x_2}, \ldots, \frac{\partial b}{\partial x_k}$ are left dependent, then by the weak algorithm (Theorem 11.2.1), without loss of generality, we may suppose that there are elements $m'_1, \ldots, m'_{k-1}$ of $U(A)$ such that $\frac{\partial b}{\partial x_k} = \sum_{j=1}^{k-1} m'_j \frac{\partial b}{\partial x_j}$. By the induction hypothesis, there exists a μ-homogeneous automorphism ψ with $\frac{\partial}{\partial x_k}(\psi(b)) = 0$ and $\psi(x_i) = x_i$ for all $i \geq k$. Therefore $\psi(b) = (\psi(a))^{(0)}$. By Lemma 12.3.3, the integer k and the element $\psi(a)$ satisfy the conditions of Proposition 12.3.2. Changing the element a by $\psi(a)$ and applying the arguments above, we may assume that there is an integer $s \leq k$ such that the elements $\frac{\partial b}{\partial x_1}, \ldots, \frac{\partial b}{\partial x_s}$ are left independent and

$$\frac{\partial(a^{(0)})}{\partial x_{s+1}} = \cdots = \frac{\partial(a^{(0)})}{\partial x_k} = 0.$$

Applying Lemma 12.3.6, we complete the proof. ■

12.4 Rank Theorems

Following [352], [354], we define the rank of an element a of a free algebra A ($\operatorname{rank}(a)$) as the minimal number of generators from X on which an automorphic image of a can depend. The rank of a system of elements $a_1, \dots, a_k$ of A is defined similarly (notation: $\operatorname{rank}(a_1, \dots, a_k)$).

For an element a of A, by M_a we denote the left $U(A)$-submodule of $U(A)$ generated by the elements $\frac{\partial a}{\partial x_1}, \dots \frac{\partial a}{\partial x_n}$. The universal multiplicative enveloping algebra $U(A)$ is a free associative algebra. The algebra $U(A)$ as a left $U(A)$-module is a free one-generated module. Any left ideal of a free associative algebra is a free module of unique rank. By $\operatorname{rank}(M_a)$ we denote the rank of the module M_a.

Lemma 12.4.1. *Let φ be an automorphism of A. Then* $\operatorname{rank}(M_{\varphi(a)}) = \operatorname{rank}(M_a)$.

Proof.

$$\frac{\partial(\varphi(a))}{\partial x_j} = \sum_{i=1}^{n} \frac{\partial(\varphi(x_i))}{\partial x_j} \varphi\left(\frac{\partial a}{\partial x_i}\right)$$

$$= \varphi\left(\sum_{i=1}^{n} \varphi^{-1}\left(\frac{\partial(\varphi(x_i))}{\partial x_j}\right) \cdot \frac{\partial a}{\partial x_i}\right) \in \varphi(M_a);$$

that is, $M_{\varphi(a)} \subseteq \varphi(M_a)$. Therefore

$$\varphi(M_a) = \varphi(M_{\varphi^{-1}(\varphi(a))}) \subseteq \varphi(\varphi^{-1}(M_{\varphi(a)})) = M_{\varphi(a)}.$$

Thus $\varphi(M_a) = M_{\varphi(a)}$ and $\operatorname{rank}(M_{\varphi(a)}) = \operatorname{rank}(M_a)$. ■

Lemma 12.4.2. *If $a \in A$, then* $\operatorname{rank}(M_a) \leq \operatorname{rank}(a)$.

Proof. Let $k = \operatorname{rank}(a)$. Then there is an automorphism φ of A such that the element $\varphi(a)$ belongs to the subalgebra generated by $x_1, x_2, \dots, x_k$, and the left $U(A)$-module $M_{\varphi(A)}$ is generated by $\frac{\partial(\varphi(a))}{\partial x_1}, \dots, \frac{\partial(\varphi(a))}{\partial x_k}$. Thus $\operatorname{rank}(M_a) = \operatorname{rank}(M_{\varphi(a)}) \leq k$. ■

Let $\mu\colon \mathbb{Z}_+^n \to \mathbb{Q}_+$ be a functional. For $\alpha > 0$, by A^α (U^α) we denote the subspace of μ-homogeneous elements of A (of $U(A)$, respectively) with the μ-degree equal to α,

$$A = \bigoplus_{\alpha \in \mathbb{Q}_+} A^\alpha, \quad U(A) = \bigoplus_{\alpha \in \mathbb{Q}_+} U^\alpha.$$

For $f \in A$ ($f \in U(A)$), by $\rho_\mu^\alpha(f)$ we denote the μ-homogeneous component of f, $\rho_\mu^\alpha(f) \in A^\alpha$ ($\rho_\mu^\alpha(f) \in U^\alpha$, respectively). Following [272], we say that an element a of A is μ-bounded if $\rho_\mu^\alpha(a) = 0$ for any $\alpha > 1$.

Let $V(\mu) = \{m \in \mathbb{Z}_+^n \mid \mu(m) \leq 1\}$. Consider the following partial ordering on the set of functionals: $\mu_1 \prec \mu_2$ if $V(\mu_1) \subset V(\mu_2)$ and $V(\mu_1) \neq V(\mu_2)$.

Lemma 12.4.3. *Let a be a μ-homogeneous element of A and* $\operatorname{rank}(M_a) < n$. *Then there exists a μ-homogeneous automorphism φ of A such that the element $\rho^1_\mu(\varphi(a))$ depends on not more than $n-1$ variables of X.*

Proof. If $\rho^1_\mu(\varphi(a))$ depends on not more than $n-1$ variables of X, then for φ we take the identical automorphism.

Suppose that $\rho^1_\mu(\varphi(a))$ depends on every variable of X. Since $\operatorname{rank}(M_a) < n$, there are not all equal to zero elements $m_1, \dots m_n$ of $U(A)$ with

$$\sum_{i=1}^{n} m_i \frac{\partial a}{\partial x_i} = 0. \tag{12.5}$$

For $i = 1, \dots, n$, we set

$$\alpha_i = \max\{\alpha \in \mathbb{Q}_+ \mid \rho^\alpha_\mu(m_i) \neq 0\},$$
$$\beta = \max\{\alpha_i - \mu(x_i) + 1 \mid i = 1, \dots, n\}$$

(if $m_i = 0$, then $\alpha_i = -1$). Since $\rho^1_\mu(a)$ depends on $x_1, \dots, x_n$, $1 - \mu(x_i) \geq 0$ for $i = 1, \dots, n$, and $\beta \geq 0$. Applying ρ^β_μ to (12.5), we get

$$\sum_{i=1}^{n} \sum_{\alpha \in \mathbb{Q}_+} \rho^{\beta-\alpha}_\mu(m_i) \cdot \rho^\alpha_\mu\left(\frac{\partial a}{\partial x_i}\right)$$
$$= \sum_{i=1}^{n} \sum_{\alpha \in \mathbb{Q}_+} \rho^{\beta-1}_\mu(m_i) \cdot \frac{\partial}{\partial x_i}(\rho^{\alpha+\mu(x_i)}_\mu(a)) = 0. \tag{12.6}$$

If $\alpha + \mu(x_i) > 1$, then taking into account that a is a μ-bounded element, we get $\rho^{\alpha+\mu(x_i)}_\mu(a) = 0$. If $\alpha + \mu(x_i) < 1$, then $\beta - \alpha \geq \alpha_i - \mu(x_i) + 1 - \alpha > \alpha_i$; that is, $\rho^{\beta-\alpha}_\mu(m_i) = 0$. Therefore, it follows from (12.6) that

$$\sum_{i=1}^{n} \rho^{\beta-1+\mu(x_i)}_\mu(m_i) \cdot \frac{\partial}{\partial x_i}(\rho^1_\mu(a)) = 0.$$

Since for some i

$$\beta - 1 + \mu(x_i) = (\alpha_i - \mu(x_i) + 1) - 1 - \mu(x_i) = \alpha_i > -1$$

and $\rho^{\beta-1+\mu(x_i)}_\mu(m_i) = \rho^{\alpha_i}_\mu(m_i) \neq 0$, it follows that elements $\frac{\partial}{\partial x_i}(\rho^1_\mu(a))$, $1 \leq i \leq n$, are left dependent. Since these elements are μ-homogeneous, there is j, $1 \leq j \leq n$, such that the element $\frac{\partial}{\partial x_j}(\rho^1_\mu(a))$ belongs to the left ideal of $U(A)$ generated by elements $\frac{\partial}{\partial x_i}(\rho^1_\mu(a))$ with $i \neq j$. By Proposition 12.3.2, there exists a μ-homogeneous automorphism φ of A such that $\varphi(\rho^1_\mu(a))$ does not depend on x_j. Now, to complete the proof it is enough to note that $\varphi(\rho^\alpha_\mu(a)) = \rho^\alpha_\mu(\varphi(a))$ for any $\alpha \in \mathbb{Q}_+$. ■

Lemma 12.4.4. *Let a be a μ-homogeneous element of A. Suppose that a depends on $x_1, \dots, x_n$. Then there exists a functional μ_0 such that $V(\mu_0) \subset V(\mu)$, a is μ_0-bounded, and the component $\rho^1_{\mu_0}(a)$ depends on $x_1, \dots, x_n$.*

Proof. Suppose that $\rho^1_\mu(a)$ depends only on $x_1, \ldots, x_k$ $(k < n)$. To prove the lemma, it is sufficient to find a functional μ_0 such that $V(\mu_0) \subset V(\mu)$, a is μ_0-bounded, and the component $\rho^1_{\mu_0}(a)$ depends on $x_1, \ldots, x_k, x_{k+1}$.

For any $t \in \mathbb{Q}_+$, let μ_t be the functional given by $\mu_t(x_i) = \alpha_i$ with $i \neq k+1$, and $\mu_t(x_{k+1}) = \mu(x_{k+1}) + t$. It is clear that $V(\mu_t) \subset V(\mu)$. Since $\rho^1_\mu(a)$ does not depend on x_{k+1}, $\mu_t(\rho^1_\mu(a)) = 1$. The element a is μ-bounded if for any monomial w having a nonzero coefficient in a such that it has the x_{k+1}-degree equal to $r > 0$, we have $\mu(w) + rt \leq 1$. Since $\rho^1_\mu(a)$ does not depend on x_{k+1}, $\mu(w) < 1$. Hence, for the element a, the property to be μ-bounded is equivalent to a system of inequalities of the form $t \leq \alpha_i$ $(\alpha_i > 0)$. Let t_0 be a maximal solution of this system. Then there exists a monomial w of the degree $r > 0$ with respect to x_{k+1} such that $\mu_{t_0}(w) = \mu(w) + rt_0 = 1$. Therefore the component $\rho^1_{\mu_{t_0}}(a)$ depends on x_{k+1}. It follows from $\mu_{t_0}(\rho^1_\mu(a)) = 1$ that $\rho^1_\mu(a)$ depends on $x_1, \ldots, x_k, x_{k+1}$. Finally, we set $\mu_0 = \mu_{t_0}$. ■

Lemma 12.4.5. *Let μ be a functional, and let a be a μ-bounded element of A. Suppose that* $\operatorname{rank}(M_a) < n$. *Then there exist an automorphism φ of A and a functional μ_0 such that $\mu_0 \prec \mu$ and the element $\varphi(a)$ is μ_0-bounded.*

Proof. By Lemma 12.4.4, we may assume that $\rho^1_\mu(a)$ depends on all variables of X. By Lemma 12.4.3, there is a μ-homogeneous automorphism φ of A such that $\rho^1_\mu(\varphi(a))$ depends at most on $n-1$ variables. We may suppose that $\rho^1_\mu(\varphi(a))$ does not depend on x_n. Since $\rho^1_\mu(a)$ depends on x_n, there exists a monomial w of the x_n-degree equal to $r > 0$ having a nonzero coefficient in a. For $t \in \mathbb{Q}_+$, we consider the functional μ_t given by $\mu_t(x_i) = x_i$ with $i \neq n$ and $\mu_t(x_n) = \mu(x_n) + t$. As in the proof of Lemma 12.4.4, we find $t_0 > 0$ such that $\varphi(a)$ is a μ_{t_0}-bounded element. We set $\mu_0 = \mu_{t_0}$. It is obvious that $V(\mu_0) \subseteq V(\mu)$. From $\mu(w) = 1$, it follows that $\mu_0(w) = \mu(w) + rt_0 > 1$. Therefore $m(w) \in V(\mu)$, but $m(w) \notin V(\mu_0)$; that is, $\mu_0 \prec \mu$. ■

Lemma 12.4.6. *Let $a \in A$,* $\operatorname{rank}(M_a) < n$. *Then, there is an automorphism φ of A such that $\varphi(a) \in H$, where H is the subalgebra of A generated by $x_1, \ldots, x_{n-1}$.*

Proof. Let d be the degree of a. We set $\mu(x_i) = \frac{1}{d}$, $i = 1, \ldots, n$. Then a is a μ-bounded element. We use the induction on the cardinality $|V(\mu)|$ of the set $V(\mu)$. If $|V(\mu)| = 1$, then $V(\mu) = \{(0, \ldots, 0)\}$, and $a = \alpha \cdot 1 \in H$ $(\alpha \in K)$. Suppose that the statement of the lemma is proved for any μ_0-bounded element a $(\mu_0 \prec \mu)$. Applying Lemma 12.4.5, we complete the proof. ■

Theorem 12.4.7 ([259]). *For any element a of A, the rank of a is equal to the rank of the left ideal M_a of $U(A)$ generated by the elements $\frac{\partial a}{\partial x_i}$, $1 \leq i \leq n$.*

Proof. By Lemma 12.4.2, $\operatorname{rank}(M_a) \leq \operatorname{rank}(a)$. Let $k = \operatorname{rank}(a)$. We may assume that a belongs to the subalgebra S of A generated by $x_1, \ldots, x_k$. By Lemma 12.4.6, the elements $\frac{\partial a}{\partial x_i}$, $1 \leq i \leq k$, are left independent over $U(S)$. Since $U(A)$ is a free $U(S)$-module, these elements are left independent over $U(A)$. Therefore $\operatorname{rank}(M_a) = k$. ■

Let e_i $(i = 1, \ldots, r)$ be the row with ith coordinate equal to 1 and other coordinates equal to 0.

Theorem 12.4.8 ([259]). *The rank of a system of elements $a_1, \ldots, a_r$ of A is equal to the rank of the left $U(A)$-module $M = M_{\{a_1,\ldots,a_r\}}$ generated by the elements $\sum_{i=1}^{r} \frac{\partial a_i}{\partial x_j} e_i$, $1 \leq j \leq n$.*

Proof. Let $s = \operatorname{rank}(M_{\{a_1,\ldots,a_r\}})$, $k = \operatorname{rank}(\{a_1, \ldots, a_r\})$. As in the proof of Lemmas 12.4.1 and 12.4.2, we see that $s = \operatorname{rank}(M_{\{\varphi(a_1),\ldots,\varphi(a_r)\}})$ for any automorphism φ of A, and $k \geq s$. Therefore we may assume that the elements a_i $(1 \leq i \leq r)$ belong to the subalgebra generated by $x_1, \ldots, x_k$. Let $Y = \{y_j \mid 1 \leq j \leq r\}$. Consider the free algebra $B = F_{\mathfrak{M}}(X \cup Y)$. It is clear that $A \subseteq B$ and $U(B)$ is a free right $U(A)$-module. Therefore $s = \operatorname{rank}_{U(A)} U(B)M$. Consider the element

$$b = a_1 y_1 + a_2 y_2 + \cdots + a_r y_r.$$

It is obvious that $\operatorname{rank}(b) \leq k + r$,

$$\frac{\partial b}{\partial x_j} = \sum_{i=1}^{k} \frac{\partial a_i}{\partial x_j} \cdot r_{y_i}, \quad 1 \leq j \leq n,$$

$$\frac{\partial b}{\partial y_s} = l_{a_s}, \quad 1 \leq s \leq r.$$

We may suppose that the elements $a_1, \ldots, a_r$ are linearly independent. Then the elements $r_{y_1}, \ldots, r_{y_r}, l_{a_1}, \ldots, l_{a_r}$ are left independent over $U(B)$. Hence

$$M_b = U(B)\left\{ \frac{\partial b}{\partial x_j} \;\middle|\; 1 \leq j \leq n \right\} \oplus U(B) l_{a_1} \oplus \cdots \oplus U(B) l_{a_r}.$$

The homomorphism f of $U(B)$ given by $f(e_i) = r_{y_i}$ induces the isomorphism

$$U(B)\left\{ \frac{\partial f}{\partial x_j} \;\middle|\; 1 \leq j \leq n \right\} \cong U(B)M.$$

Thus, $\operatorname{rank}_{U(B)} M_b = s + r$. By Theorem 12.4.7, $\operatorname{rank}(b) = s + r \leq k + r$; that is, $s = k$. ■

Now we consider rank theorems for free Lie algebras and superalgebras.

In all of what follows, we denote $L_X = L(X)$ (the free color Lie superalgebra) in the case where $\operatorname{char} K = 0$, and $L_X = L^p(X)$ (the free color Lie p-superalgebra) in the case where $\operatorname{char} K = p > 2$.

Theorem 12.4.9 ([272, 273]). *Let h be a G-homogeneous element of L_X. Then* $\operatorname{rank}(h)$ *is equal to the rank of the left ideal of $K\langle X\rangle$ generated by the elements $\{\frac{\partial h}{\partial x} \mid x \in X\}$ (as a free left $K\langle X\rangle$-module).*

Theorem 12.4.10 ([272, 273]). *Let $h_1, \ldots, h_k$ be G-homogeneous elements of L_X. Then the rank of the system $\{h_1, \ldots, h_k\}$ is equal to the rank of the left $K\langle X\rangle$-submodule of the $K\langle X\rangle$-module*

$$K\langle X\rangle^k = K\langle X\rangle e_1 \oplus \cdots \oplus K\langle X\rangle e_k$$

generated by the elements

$$\left\{ \sum_{i=1}^{k} \frac{\partial h_i}{\partial x} e_i \;\middle|\; x \in X \right\}.$$

As was proved by U. U. Umirbaev in [391], the statements of Theorems 12.4.9 and 12.4.10 take place for the free group F (instead of $K\langle X\rangle$ it is necessary to consider the group algebra of F over a field K; this algebra is a fir).

Problem 12.4.11. Find criteria for an element of a polynomial or a free associative algebra to have a given rank and an algorithm to determine the rank of an element.

Theorems 12.4.7–12.4.10 (together with the weak algorithm) give us an effective algorithm to find the rank of a system of elements of a free algebra of a Schreier variety of algebras. For a homogeneous element of a free Lie algebra, an algorithm to find the rank was constructed by V. Shpilrain [354].

A. A. Mikhalev and A. A. Zolotykh [272, 275, 280] obtained algorithms to realize the rank of a system of elements in free Lie (p-)(super)algebras (i.e., algorithms to construct a concrete automorphism such that the images of elements depend on a minimal possible number of free generators). For free ((anti)commutative) nonassociative algebras, such algorithms were constructed by K. Champagnier [66].

12.5 Primitive Elements

We recall that a system of elements of a free algebra F is said to be primitive if it is a subset of some set of free generators of F.

Let $X = \{x_1, \ldots, x_n\}$. Let also A be the free algebra with the set X of free generators of the variety $\mathfrak{M}_0$ (the variety of all algebras), $\mathfrak{M}_1$ (the variety of all commutative algebras, $\operatorname{char} K \neq 2$), or $\mathfrak{M}_2$ (the variety of all anticommutative algebras).

12.5.1 Primitive elements in free nonassociative algebras

Theorem 12.5.1 ([259]). *A system $a_1, \dots, a_r$ of elements of A is primitive if and only if the matrix $(\partial(a_1), \dots, \partial(a_r))$ is left invertible over $U(A)$. In particular, an element a of A is primitive if and only if there are $m_1, \dots, m_n \in U(A)$ such that $\sum_{i=1}^{n} m_i \frac{\partial a}{\partial x_i} = 1$.*

Proof. Let e_i $(i = 1, \dots, r)$ be the row with ith coordinate equal to 1 and other coordinates equal to 0. By $M_{\{a_1,\dots,a_r\}}$ we denote the left $U(A)$-module generated by the elements $\sum_{i=1}^{r} \frac{\partial a_i}{\partial x_j} e_i$, $1 \le j \le n$. If the matrix $(\partial(a_1), \dots, \partial(a_r))$ is left invertible over $U(A)$, then

$$M_{\{a_1,\dots,a_r\}} = U(A)e_1 \oplus U(A)e_2 \oplus \cdots \oplus U(A)e_r = \bigoplus_{i=1}^{r} U(A)e_i. \qquad (12.7)$$

By Theorem 12.4.8, $\operatorname{rank}(a_1, \dots, a_r) = r$. Moreover, it follows from (12.7) that for any automorphism φ of A we have

$$M_{\{\varphi(a_1),\dots,\varphi(a_r)\}} = \bigoplus_{i=1}^{r} U(A)e_i.$$

We may assume that $a_1, \dots, a_r$ belong to the subalgebra S of A generated by $x_1, \dots, x_r$. Let ψ be an endomorphism of S given by $\psi(x_i) = a_i$. It follows from (12.7) that the Jacobian matrix of ψ is invertible. Therefore φ is an automorphism. The inverse statement is obvious. ■

Theorem 12.5.2 ([259]). *For a system of elements $a_1, \dots, a_r$ of A, there is an algorithm to decide whether this system is primitive or not.*

Proof. For one element a of A, we consider the left ideal M_a of A. Using elementary reductions, we construct the standard Gröbner–Shirshov basis of this ideal. The cardinality of this basis is exactly the rank of a. The element a is primitive if and only if $\operatorname{rank}(a) = 1$ and the standard Gröbner–Shirshov basis of M_a consists only of the unity element.

In the general case, the rank of the system $a_1, \dots, a_k$ is equal to the left rank of the matrix $(\partial(a_1), \dots, \partial(a_k))$. Using (left) elementary transformations of rows, we find this rank. The system is primitive if and only if this matrix is left invertible. ■

12.5.2 Primitive elements in free Lie superalgebras

Now we consider primitive systems of elements of free color Lie (p-)superalgebras.

Let L be the free color Lie superalgebra $L(X)$ or the free color Lie p-superalgebra $L^p(X)$. For $a \in L$ we denote by $\partial(a) = \partial_X(a)$ the column $(\frac{\partial a}{\partial x_1}, \dots, \frac{\partial a}{\partial x_n})^{\mathrm{T}}$. For an endomorphism φ of L by $J_k(\varphi)$, $k \le n$, we consider

the $(k \times k)$-matrix

$$J_k(\varphi) = \begin{pmatrix} \frac{\partial \varphi(x_1)}{\partial x_1} & \cdots & \frac{\partial \varphi(x_k)}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial \varphi(x_1)}{\partial x_k} & \cdots & \frac{\partial \varphi(x_k)}{\partial x_k} \end{pmatrix},$$

and we say that $J_k(\varphi)$ is the kth Jacobian matrix of φ. If $k = n$, then $J(\varphi) = J_n(\varphi)$ is called the Jacobian matrix of φ.

The following theorem gives a positive solution of the Jacobian problem for free color Lie (p-)superalgebras.

Theorem 12.5.3 ([249]). *Let K be a field and $X = \{x_1, \ldots, x_n\}$. An endomorphism φ of the free color Lie (p-)superalgebra L is an automorphism if and only if the Jacobian matrix $J(\varphi)$ is invertible over $A(X)$. Moreover, $J(\varphi)^{-1} = \varphi(J(\varphi^{-1}))$.*

Note that a square matrix over a free associative algebra is left invertible if and only if it is right invertible. It follows from the fact that a free associative algebra can be embedded into a skew field (see the monographs [80, 81, 328]). The Jacobian conjecture for free Lie algebras was proved by U. U. Umirbaev [387], C. Reutenauer [312], and V. Shpilrain [351]. More general situations for Lie algebras were considered by U. U. Umirbaev [387] and V. Shpilrain [351]. The Jacobian conjecture for free Lie (p-)superalgebras was proved by A. A. Mikhalev [249]. The Jacobian conjecture for free Lie algebras over rings was proved by A. A. Mikhalev and A. A. Zolotykh [274]. The Jacobian conjecture for free nonassociative algebras and free (anti)commutative (nonassociative) algebras was proved by A. V. Yagzhev in [406] and for other types of free algebras with the Nielsen–Schreier property by U. U. Umirbaev [388].

Note that for the composition of endomorphisms φ and ψ of $L(X)$ (of $L^p(X)$), the Jacobian matrix $J(\psi \circ \varphi)$ is equal to $J(\psi)\psi(J(\varphi))$.

It is possible also to give a solution of the Jacobian problem for Lie superalgebras in the following form (the exposition of this result for Lie algebras was given by U. U. Umirbaev):

Theorem 12.5.4. *Let $X = \{x_1, \ldots, x_n\}$, $Y = \{y_1, \ldots, y_n\}$, $d(x_i) = d(y_i)$, $X \cap Y = \varnothing$, $L = L(X)$ $(L = L^p(X))$, $L' = L(X \cup Y)$ $(L' = L^p(X \cup Y))$, and let φ be an endomorphism of L, $\varphi(x_i) = f_i$. Consider the endomorphism φ' of L' given by*

$$\varphi'(x_i) = f_i', \quad \varphi'(y_i) = y_i, \quad 1 \leq i \leq n,$$

where f_i' are X-linear parts of the elements

$$f_i|_{\substack{x_1 = x_1 + y_1, \\ \cdots \\ x_n = x_n + y_n}}, \quad i = 1, \ldots, n.$$

Then φ' is an automorphism of L' if and only if φ is an automorphism of L.

Theorem 12.5.3 gives an effective procedure to recognize automorphisms of free Lie algebras and superalgebras among endomorphisms. Another algorithm follows from Theorem 11.1.1.

Let $X = \{x_1, \dots, x_n\}$. For the free associative algebra $K\langle X\rangle$, denote by $K\langle X\rangle^e$ the tensor product $K\langle X\rangle \otimes_K K\langle X\rangle$ with the multiplication given by $(a\otimes b)(c\otimes d) = ac\otimes db$. It is clear that $K\langle X\rangle^e$ is the universal multiplicative enveloping algebra for $K\langle X\rangle$. Let

$$I_A = \bigoplus_{i=1}^{n} (K\langle X\rangle^e)_i = \bigoplus_{i=1}^{n} (K\langle X\rangle \cdot dx_i \cdot K\langle X\rangle)_i$$

be the direct sum of n copies of $K\langle X\rangle^e$, $(K\langle X\rangle^e)_i = K\langle X\rangle \cdot dx_i \cdot K\langle X\rangle$, $(a\otimes b)_i = a\cdot dx_i \cdot b$. The universal derivation of $K\langle X\rangle$ is the K-linear mapping $D\colon K\langle X\rangle \to I_A$ given by $D(x_i) = 1 \cdot dx_i \cdot 1$, $D(ab) = D(a)\cdot b + a\cdot D(b)$, $D(1) = 0$. For any $a \in K\langle X\rangle$, the element $D(a)$ has the unique presentation in the form $D(a) = a_1 + \cdots + a_n$, $a_i \in (K\langle X\rangle^e)_i$. The component $a_i = \frac{\partial a}{\partial x_i}$ is the partial derivative of a on x_i.

If we consider the natural homomorphism of associative algebras with the identity elements $\varphi\colon K\langle X\rangle^e \to K[X]$ (where $K[X]$ is the polynomial algebra), $\varphi(a\otimes b) = ab$, then the images of partial derivatives of elements of $K\langle X\rangle$ are the usual partial derivatives of elements of $K[X]$.

If $X = \{x_1, \dots, x_n\}$ and φ is an endomorphism of $K\langle X\rangle$, then φ is an automorphism if and only if the Jacobian matrix

$$\left(\frac{\partial \varphi(x_j)}{\partial x_i}\right), \quad 1 \le i, j \le n,$$

is invertible over $K\langle X\rangle^e$. This result for $n = 2$ was obtained by W. Dicks and J. Lewin [96] and for arbitrary n by A. H. Schofield [328]. A. A. Mikhalev and A. A. Zolotykh proved this result for free associative algebras over an associative commutative ring [276].

The statement of the Jacobian conjecture fails for $K\langle X\rangle$ if we use Lie partial derivatives. For example, let $X = \{x_1, x_2\}$, $\varphi(x_1) = x_1 + x_2x_1x_2$, $\varphi(x_2) = x_2$. Then

$$J(\varphi) = \begin{pmatrix} 1 & 0 \\ x_1x_2 & 1 \end{pmatrix}$$

is invertible, but at the same time φ is not an automorphism. But in the case $n = 2$, V. Shpilrain [350], using Dicks' commutator test, proved that φ is an automorphism if and only if the matrix

$$\begin{pmatrix} \frac{\partial}{\partial x_2}\varphi(x_2) & -\frac{\partial}{\partial x_2}\varphi(x_1) \\ -\frac{\partial}{\partial x_1}\varphi(x_2) & \frac{\partial}{\partial x_1}\varphi(x_1) \end{pmatrix} \begin{pmatrix} \varphi(x_1)\frac{\partial}{\partial x_1} & \varphi(x_1)\frac{\partial}{\partial x_2} \\ \varphi(x_2)\frac{\partial}{\partial x_1} & \varphi(x_2)\frac{\partial}{\partial x_2} \end{pmatrix}$$

is a nonzero scalar matrix.

The following results give matrix criteria for a system of elements of free Lie (p-)superalgebras to be primitive.

Theorem 12.5.5 ([272, 273]). *Let h be a G-homogeneous element of L_X. Then the following conditions are equivalent:*

(i) *The element h is primitive.*

(ii) *There exist elements $m_1, \dots, m_n \in K\langle X\rangle$ such that*

$$\sum_{i=1}^{n} m_i \frac{\partial h}{\partial x_i} = 1.$$

Note that the statement of Theorem 12.5.5 does not take place for free Lie algebras over fields of positive characteristic. A. A. Mikhalev, U. U. Umirbaev, and A. A. Zolotykh constructed a series of such examples in [261, 262]. We show one such example. Let K be a field, $\operatorname{char} K = p > 2$, $X = \{x, y, z\}$, $L(X)$ the free Lie algebra, and $h = x + [y, z] + (\operatorname{ad} x)^p(z) \in L(X)$. Then h is not a primitive element of $L(X)$, but at the same time the rank of the left ideal of $K\langle X\rangle$ generated by the elements $\frac{\partial h}{\partial x}$, $\frac{\partial h}{\partial y}$, $\frac{\partial h}{\partial z}$ is equal to 1 (h is a primitive element of $L^p(X)$ but not of $L(X)$). Indeed, suppose that h is a primitive element of $L(X)$. Then there exist primitive elements f_1, f_2 of $L(X)$ such that $\{f_1, f_2, h\}$ is a primitive system of elements, $L(X) = L(\{f_1, f_2, h\})$. By Theorem 11.1.1, we may assume that $\ell(f_1) \le \ell(f_2) < \ell(h)$ and that the leading part h° of h is a Lie polynomial on leading parts f_1°, f_2° of elements f_1, f_2, respectively. Since $h^\circ = (\operatorname{ad} x)^p(z)$, we may assume $f_1^\circ = \alpha x$, $0 \ne \alpha \in K$. Therefore $f_1 = \alpha x$, and

$$h - \frac{1}{\alpha} f_1 = [y, z] + (\operatorname{ad} x)^p(z)$$

is a primitive element. It gives a contradiction with the fact that any set of free generators of $L(X)$ forms a basis of $L(X)$ modulo $[L(X), L(X)]$.

Consider now the partial derivatives of h:

$$\frac{\partial h}{\partial x} = 1 + x^{p-1} z, \quad \frac{\partial h}{\partial y} = z, \quad \frac{\partial h}{\partial z} = -y - x^p.$$

Setting $m_1 = 1$, $m_2 = -x^{p-1}$, $m_3 = 0$, we get the equality

$$m_1 \frac{\partial h}{\partial x} + m_2 \frac{\partial h}{\partial y} + m_3 \frac{\partial h}{\partial z} = 1.$$

Let I be the ideal of $L(X)$ generated by h, $L = L(X)/I$. Since h is not a primitive element of $L(X)$, L is not a free Lie algebra ([191]; see also Section 12.5.3). But the universal enveloping algebra of L is a free associative algebra of rank 2. Indeed, $U(L) = K\langle X\rangle / J$, where J is the ideal of $K\langle X\rangle$ generated by h. At the same time h is a primitive element of $K\langle X\rangle$: $h = x + [y + x^p, z]$, it can be obtained from x by applying two elementary automorphisms. In particular, the cohomological dimension of the Lie algebra L is equal to 1 [261, 262, 275]. It shows that there is no analog of the Stallings–Swan theorem (that groups of cohomological dimension 1 are free [372, 381]) for free Lie algebras over fields of prime characteristic.

Problem 12.5.6. Let $\operatorname{char} K = 0$. Is it true that a Lie K-algebra L is free if and only if its universal enveloping algebra $U(L)$ is a free associative K-algebra?

Problem 12.5.7. Let $\operatorname{char} K = 0$. Is it true that a Lie K-algebra L is free if and only if its cohomological dimension is equal to 1?

This problem was solved in the affirmative for two-generated Lie algebras by G. L. Feldman [127]. Some necessary and sufficient conditions for Lie algebras with one defining relation to have cohomological dimension 1 were obtained by A. V. Sereguine [333].

Theorem 12.5.8 ([272, 273]). *Let $h_1, \dots, h_k$ be G-homogeneous elements of L_X. Then the following conditions are equivalent:*

(i) *The system $\{h_1, \dots, h_k\}$ is primitive.*

(ii) *There exist elements $m_{ij} \in K\langle X\rangle$, $i = 1, \dots, k$, $j = 1, \dots, n$, such that for all $r, s = 1, \dots, k$*

$$\sum_{i=1}^{n} m_{ri} \frac{\partial h_s}{\partial x_i} = \delta_{rs};$$

i.e., the $(n \times k)$-matrix $(\frac{\partial h_j}{\partial x_i})$ is left invertible.

Theorems 12.5.5 and 12.5.8 give us an effective algorithm to decide whether a system of elements of a free color Lie (p-superalgebra) is primitive or not. Moreover, A. A. Mikhalev and A. A. Zolotykh [272, 275, 278, 280] constructed an algorithm to construct a complement of a primitive system of elements with respect to a free generating set of the free Lie (p-)superalgebra. Based on Theorem 12.5.1, K. Champagnier [66] constructed a similar algorithm for free ((anti)commutative) nonassociative algebras.

Problem 12.5.9. Are the assertions of Theorems 12.5.5 and 12.5.8 valid for free Lie rings?

Problem 12.5.10. Find criteria for an element of a polynomial or a free associative algebra to be primitive and an algorithm to determine primitive elements.

V. Shpilrain and J.-T. Yu [359, 360] constructed algorithms to recognize coordinate polynomials of a polynomial algebra of rank 2 (primitive elements of a free associative algebra of rank 2, respectively) over a field of characteristic zero; see Chapter 9.

Problem 12.5.11. Is it true that an element a of the free associative algebra $K\langle x, y\rangle$ is primitive if and only if there are elements b_1, b_2 of the algebra $K\langle x, y\rangle^e$ such that $b_1 \frac{\partial a}{\partial x} + b_2 \frac{\partial a}{\partial y} = 1 \otimes 1$?

Theorem 12.5.1 for a single primitive element of a free group was proved by W. Dicks and M. J. Dunwoody [95, Corollary IV.5.3], and for a system of elements of a free group a result similar to Theorem 12.5.8 was obtained by U. U. Umirbaev [389]. An algorithm to recognize primitive elements of free groups was constructed by J. H. C. Whitehead in [399, 400] (in fact, he solved a more general automorphic conjugacy problem; see [227]).

12.5.3 The Freiheitssatz and primitive elements

In this section, Theorem 12.5.15 gives a nonmatrix criterion for an element to be primitive.

Proposition 12.5.12. *Let I be a nonzero ideal of A such that the factor algebra A/I is a free algebra of the variety $\mathfrak{M}$ with k free generators. Then there is a primitive system of elements $g_1, \dots, g_{n-k}$ of A such that it generates the ideal I.*

Proof. Let $\varphi\colon A \to B = F_{\mathfrak{M}}\langle y_1, \dots, y_k\rangle$ be a surjective homomorphism, $\ker(\varphi) = I$. We set $f_i = \varphi(x_i)$, $1 \le i \le n$. Consider the system of elements $f_1, f_2, \dots, f_n$ of the algebra B. Since the variety $\mathfrak{M}$ has the Nielsen property (Theorem 11.1.1), by a finite sequence of elementary transformations we can transform this system to $y_1, \dots, y_k, 0, \dots, 0$. Applying the same sequence of transformations to $x_1, \dots, x_n$, we get a new set of free generators $p_1, \dots, p_k, q_1, \dots, q_{n-k}$ of A. It is clear that $\varphi(p_i) = y_i$, $\varphi(q_j) = 0$ for all i, j. Thus the ideal I is generated by $q_1, \dots, q_{n-k}$. ■

An algebra S defined by n generators and m relations with $n > m$ in a fixed variety is said to satisfy Lyndon's condition if among given generators there are $n - m$ elements generating a free subalgebra in this variety. O. G. Kharlampovich [175] proved that free algebras of the variety of all Lie algebras and of the variety of all l-step solvable Lie algebras satisfy Lyndon's condition.

Theorem 12.5.13 (Freiheitssatz, [347, 416]). *Suppose that an element a of A depends on a free generator $x \in X$. Let (a) be the ideal of A generated by (a). Then the set $X \setminus x$ generates a free algebra of the variety $\mathfrak{M}$ in the factor algebra $A/(a)$. In other words, $F(X \setminus x) \cap (a) = 0$.*

The Freiheitssatz in group theory is due to W. Magnus [229]. For free nonassociative algebras, the Freiheitssatz was proved by A. I. Zhukov [416] and for free commutative and anticommutative nonassociative algebras by A. I. Shirshov [347]. For Lie algebras, this result was obtained by A. I. Shirshov [348]. In associative algebras, these problems were solved in the case of the field of zero characteristic by L. G. Makar-Limanov [234] and in the case of a homogeneous relation by M. Hedges in [150]. We mention also papers [92], [141], and [215] devoted to the study of associative algebras with one defining relation.

An element u of a free group F is a root of an element $w \in F$ if w belongs to the normal closure of u in F. W. Magnus [229] showed that if w is primitive, then (to within conjugacy and inversion) the only root of w is the trivial one, namely w itself. By analogy, if u, w are nonzero elements of a free algebra $F(X)$, then we say that u is a root of an element $w \in F$ if w belongs to the ideal of $F(X)$ generated by u. Let $F(X)$ be a free ((anti)commutative) nonassociative algebra, a free Lie algebra over a field of zero characteristic. Suppose that w is a primitive element of $F(X)$. Then it follows from the Freiheitssatz that all roots of w are trivial (i.e., of the form αw, $0 \neq \alpha \in K$). Note that if the field K is constructive and has an algorithm for square root extraction, then there is an algorithm to decide whether an even element of a free color Lie superalgebra is a square of some odd element and, if so, to find a square root [33, Chapter 2, Theorem 2.14].

For more facts on the application of the Freiheitssatz, we refer to the review article [178].

Problem 12.5.14. Does the Freiheitssatz take place for Lie p-algebras and color Lie p-superalgebras?

One can find some particular examples of positive answers to the Freiheitssatz for free Lie (p-)superalgebras in [33, 246, 251, 275].

Theorem 12.5.15. *Let a be a nonzero element of A, (a) the ideal of A generated by (a). Then a is a primitive element if and only if the factor algebra $A/(a)$ is a free algebra of the variety $\mathfrak{M}$.*

Proof. Let $A/I \cong F_{\mathfrak{M}}\langle y_1, \ldots, y_k\rangle$. By Proposition 12.5.12, we may assume that the ideal (a) is generated by $x_1, \ldots, x_{n-k}$. By Theorem 12.5.13, $n-k = 1$, and $a = \alpha x_1$, $0 \neq \alpha \in F$.

If a is a primitive element of A, then obviously $A/(a)$ is a free algebra of the variety $\mathfrak{M}$. ■

The result similar to Theorem 12.5.15 was proved for free Lie algebras by G. P. Kukin in [191] and for two-variable polynomial algebras over a field of zero characteristic by S. S. Abhyankar and T. T. Moh in [10]. This statement is also true for free groups; we refer to [227]. For free associative algebras of rank greater than 2, this statement does not hold; see Theorem 9.3.1. It does hold for the free associative algebra of rank 2; see Proposition 8.3.3.

It follows from Theorem 12.5.15 that if u and v are elements of A, and $A/(u)$ and $A/(v)$ are isomorphic free algebras, then there is an automorphism φ of A such that $\varphi(u) = v$ (actually, u and v are primitive elements). It turns out that there is no generalization of this result for arbitrary elements u and v.

Theorem 12.5.16 ([254]). *Let K be a field, $L = L(x, y, z)$ the free Lie algebra over K with the set $\{x, y, z\}$ of free generators. Let*

$$u = x - [[x, y], [y, z]], \quad v = x + [[[y, z], x], y],$$

and let (u) and (v) be the ideals of L generated by the elements u and v, respectively. Then $L/(u) \cong L/(v)$, but there is no automorphism φ of L such that $\varphi(u) = v$.

Proposition 12.5.17 ([254]). *Let K be a field, $L = L(x, y)$ the free Lie algebra over K with the set $\{x, y\}$ of free generators. Let*

$$u = x - [[[x, y], y], [x, y]], \quad v = x - [[[x, y], x], y],$$

and let (u) and (v) be the ideals of L generated by the elements u and v, respectively. Then $L/(u) \cong L/(v)$, but there is no automorphism φ of L such that $\varphi(u) = v$.

Corollary 12.5.18. *There are isomorphic one-relator Lie algebras $L/(u)$ and $L/(v)$ such that the isomorphism is not induced by any automorphism of the ambient free Lie algebra L. Or, equivalently, there is no automorphism of L that takes the ideal (u) to (v).*

Problem 12.5.19. Does the statement of Theorem 12.5.15 take place for free Lie p-algebras and free color Lie p-superalgebras?

In [14] S. A. Agalakov showed that a Lie algebra with one defining relation need not be residually finite.

12.6 Primitive Elements and Endomorphisms

In this section, we consider automorphic orbits of primitive elements of the free algebra A under the action of endomorphisms.

For any element a of A, by a° we denote the leading μ-homogeneous component of a, where μ is a generalized degree function. Recall that a system of elements $a_1, \ldots, a_k$ is said to be reduced if for any $i = 1, \ldots, k$ the component a_i° does not belong to the subalgebra generated by a_j° with $j \neq i$.

Proposition 12.6.1. *Let φ be an endomorphism of A sending primitive elements to primitive elements, $a_i = \varphi(x_i)$, $1 \leq i \leq n$, $\mathfrak{M} \neq \mathfrak{M}_2$ for $n = 2$. Suppose that the system $a_1, \ldots, a_{n-1}$ is reduced. Then:*

(i) *There is a μ-homogeneous element h of H with $\operatorname{rank}(h) = n - 1$, $\mu(h(a_1^\circ, \ldots, a_{n-1}^\circ)) > \mu(a_n^\circ)$.*

(ii) $\operatorname{rank}(a_1^\circ, \ldots, a_{n-1}^\circ) < n$.

(iii) *There is a μ-homogeneous automorphism ψ of A such that elements $\psi(a_1^\circ), \ldots, \psi(a_n^\circ)$ do not depend on some variable x_j of X.*

Proof. Let $h = x_1 r_{x_2} \ldots r_{x_{n-1}} r_{x_1}^s$, where $s \cdot \mu(x_1) > \mu(a_n^\circ)$. It is clear that $h = 0$ if and only if $n = 2$ and $\mathfrak{M} = \mathfrak{M}_2$. It is easy to see that the element h satisfies the condition (i).

(ii). The element $f = x_n + h(x_1, \dots, x_{n-1})$ is primitive. Then by the conditions of the lemma, the element $g = \varphi(f)$ is also primitive. By Theorem 12.5.1, there are elements m_i, $1 \le i \le n$, of $U(A)$ such that $\sum_{i=1}^{n} m_i \frac{\partial a}{\partial x_i} = 1$. Since $g = a_n + h(a_1, \dots, a_{n-1})$,

$$\sum_{i=1}^{n} m_i \frac{\partial a_n}{\partial x_i} + \sum_{j=1}^{n-1} \left(\sum_{i=1}^{n} m_i \frac{\partial a_j}{\partial x_i} \right) \cdot \frac{\partial h}{\partial x_j}(a_1, \dots, a_{n-1}) = 1.$$

Considering the component of the degree

$$r + \mu(h(a_1^\circ, \dots, a_{n-1}^\circ)), \quad \text{where} \quad r = \max\{\mu(m_i) - \mu(x_i)\},$$

we get

$$\sum_{j=1}^{n-1} \left(\sum_{i=1}^{n} m_i' \frac{\partial a_j^\circ}{\partial x_i} \right) \frac{\partial h}{\partial x_j}(a_1^\circ, \dots, a_{n-1}^\circ) = 0, \tag{12.8}$$

where m_i' is the component of m_i of the degree $r + \mu(x_i)$. By Theorem 11.1.1, since the system $a_1, \dots, a_{n-1}$ is reduced, it forms a set of free generators of the subalgebra S of A that it generates. It follows from $\operatorname{rank}(h) = n - 1$ that the elements $\frac{\partial h}{\partial x_j}(a_1^\circ, \dots, a_{n-1}^\circ)$, $1 \le j \le n-1$, are left independent over $U(S)$. Since $U(A)$ is a free left $U(S)$-module, it follows from (12.8) that

$$\sum_{i=1}^{r} m_i' \frac{\partial a_j^\circ}{\partial x_i} = 0, \quad 1 \le j \le n.$$

By Theorem 12.4.8, $\operatorname{rank}(a_1^\circ, \dots, a_{n-1}^\circ) < n$.

(iii). Fix $t \in \mathbb{Q}$ such that

$$t > \max\{\mu(x_i), \mu(a_j^\circ) \mid 1 \le i \le n,\ 1 \le j \le n-\}.$$

Let $Y = \{y_1, \dots, y_{n-1}\}$, $\mu(y_i) = 2t - \mu(a_i^\circ)$, $1 \le i \le n-1$, $B = F_{\mathfrak{M}}(X \cup Y)$. Consider the homogeneous element

$$b = a_1^\circ y_1 + a_2^\circ y_2 + \cdots + a_{n-1}^\circ y_{n-1} \in B.$$

As in the proof of Theorem 12.4.8, elements $\frac{\partial b}{\partial x_1}, \dots, \frac{\partial b}{\partial x_n}$ are left dependent over $U(B)$. Since these elements are homogeneous, there is j with $\frac{\partial b}{\partial x_j} \in \sum_{i \ne j} U(B) \frac{\partial b}{\partial x_i}$. By Proposition 12.3.2, there is a μ-homogeneous automorphism ψ of B such that $\psi(y_i) = y_i$, $1 \le i \le n-1$, and an element $\psi(b)$ does not depend on x_j. Since $\mu(x_i) < t < \mu(y_i)$ for any i, j, the element $\psi(x_i)$ does not depend on y_j. Thus $\psi(x_i) \in A$, and the restriction of ψ on A is a desirable automorphism. ■

Theorem 12.6.2 ([259]). *Let φ be an endomorphism of A such that for any primitive element a of A the element $\varphi(a)$ is primitive. Then φ is an automorphism of A.*

Proof. We may suppose that $a_i = \varphi(x_i) = x_i + b_i$, $1 \leq i \leq n$, where b_i are linear combinations of monomials of degree not less than 2. If $n = 2$ and $\mathfrak{M} = \mathfrak{M}_2$, then primitive elements of A have the form $\alpha x_1 + \beta x_2$, where $\alpha, \beta \in F$, $(\alpha, \beta) \neq (0, 0)$. In this case, $\psi(x_i) = x_i$ and φ is an automorphism.

Suppose that if $n = 2$, then $\mathfrak{M} \neq \mathfrak{M}_2$. Consider the set of functionals

$$\{\mu \mid \text{there is an automorphism } \psi_\mu \text{ such that } \psi_\mu(a_1), \ldots \psi_\mu(a_{n-1}) \text{ are } \mu\text{-bounded}\}.$$

Let μ be a minimal element of this set with respect to the ordering $\prec$. Considering the composition $\psi \circ \varphi$, we may suppose that elements $a_1, \ldots, a_{n-1}$ are μ-bounded. We show that there is j such that $a_1, \ldots, a_{n-1}$ do not depend on x_j. Assume the contrary. As in the proof of Lemma 12.4.4, we find a functional μ_0 such that $\mu_0 \preceq \mu$ and the components $\rho^1_{\mu_0}(a_1^\circ), \ldots, \rho^1_{\mu_0}(a_{n-1}^\circ)$ depend on every $x \in X$. Using point (iii) of Proposition 12.6.1 and the proof of Lemma 12.4.5, we construct a functional μ_1 and an automorphism ψ of A such that $\mu_1 \prec \mu_0$ and elements $\psi(a_1), \ldots, \psi(a_{n-1})$ are μ_1-bounded. We have come to a contradiction with the choice of μ. Hence $a_1, \ldots, a_{n-1}$ do not depend on x_j. We may assume that $j = n$. Then $a_1, \ldots, a_{n-1} \in H$, and the restriction of φ' on H is an endomorphism of H preserving the primitivity of elements. Using the induction on n, we may assume that φ' is an automorphism of H, $\varphi'(x_i) = x_i$ with $i \leq n$, and $\varphi(x_n)$ belongs to the ideal of A generates by x_n. Since the element $b = \varphi(x_n)$ is primitive, $A/(b) \cong H \cong A/(x_n)$, where (b) and (x_n) are ideals of A generated by b and x_n, respectively. It follows that $(b) = (x_n)$. By Theorem 12.5.13, $\varphi(x_n) = \alpha x_n$, $0 \neq \alpha \in K$. Thus, φ is an automorphism of A. ■

Now we describe the situation in free Lie algebras and superalgebras. Let $L_X = L(X)$ (the free color Lie superalgebra) in the case where $\operatorname{char} K = 0$ and $L_X = L^p(X)$ (the free color Lie p-superalgebra) in the case where $\operatorname{char} K = p > 2$.

Theorem 12.6.3 ([269, 271]). *Let $X = \{x_1, \ldots, x_n\}$, and let φ be an endomorphism of L_X such that for any primitive element u of L_X the element $\varphi(u)$ is also primitive. Then φ is an automorphism of L_X.*

Problem 12.6.4. Let φ be an endomorphism of the free Lie algebra $L(X)$ over a field of positive characteristic such that for any primitive element h the image $\varphi(h)$ is a primitive element. Is it true that φ is an automorphism?

Problem 12.6.5. Let φ be either an endomorphism of $K[X]$ (or of $K\langle X\rangle$) or of the free group $F(X)$ such that for any primitive element h the image $\varphi(h)$ is a primitive element. Is it true that φ is an automorphism?

This problem has a close connection with the Jacobian conjecture for free algebras and groups and was discussed for free groups by V. Shpilrain in [352]. He pointed out that this problem is open (only in the

case $n = 2$ was it solved in the positive way, by V. Shpilrain [356] and S. V. Ivanov [154]). Under some additional assumptions, Problem 12.6.5 for free groups was solved by S. V. Ivanov in [154]. D. Lee [205] settled the problem for an arbitrary rank n. A. van den Essen and V. Shpilrain in [124] obtained an analogous result for a primitive element h of the polynomial algebra in two variables (and of the free associative algebra of rank 2). Z. Jelonek [161] proved the statement of Theorem 12.6.2 for polynomial algebras over the field of complex numbers.

Now we consider the images of linear combinations of free generators under an endomorphism and propose some problems. In Theorem 12.6.3, it is impossible to consider only images of such nonzero G-homogeneous linear combinations, as the following example shows. Let $X = \{x, y, z\}$, $G = \mathbb{Z}_2$, $d(x) = 0$, $d(y) = d(z) = 1$, $L = L(X)$ the free Lie superalgebra, and φ the endomorphism of L given by

$$\varphi(x) = x + [y, z] + [x, z, z], \quad \varphi(y) = y, \quad \varphi(z) = z.$$

Then it is clear that the image under φ of any $\mathbb{Z}_2$-homogeneous nonzero linear combinations of x, y, and z is a primitive element, and at the same time φ is not an automorphism of L.

Moreover, even in the case of free Lie algebras, it is impossible in Theorem 12.6.3 to consider only images of linear combinations of elements of the free generating set. Indeed, the following theorem takes place.

Theorem 12.6.6 ([271]). *Suppose that $n \geq 3$, $X = \{x_1, \ldots, x_n\}$, the field K is not algebraically closed, and $L = L(X)$ ($L = L^p(X)$) is the free Lie (p-)algebra. Then there exists an endomorphism φ of L such that φ is not an automorphism of L and at the same time for any nonzero linear combination a of elements of X the image $\varphi(a)$ is a primitive element.*

The situation in free associative algebras and in polynomial algebras is the same, as the following theorem shows.

Theorem 12.6.7 ([268]). *Suppose that K is a not algebraically closed field, $n \geq 3$, $X = \{x_1, \ldots, x_n\}$, and $K[X]$ is the polynomial algebra over K. Then there exists an endomorphism φ of $K[X]$ such that φ is not an automorphism of $K[X]$ and at the same time for any nonzero linear combination a of elements of X the image $\varphi(a)$ is a coordinate polynomial.*

Theorem 12.6.8 ([268]). *Suppose that K is a not algebraically closed field, $n \geq 3$, $X = \{x_1, \ldots, x_n\}$, and $K\langle X\rangle$ is the free associative algebra over K. Then there exists an endomorphism φ of $K\langle X\rangle$ such that φ is not an automorphism of $K\langle X\rangle$ and at the same time for any nonzero linear combination a of elements of X the image $\varphi(a)$ is a primitive element.*

But for algebras of rank 2 over a field of zero characteristic, the situation is different. For two-variable polynomial algebras [68] (for free associative algebras of rank 2 [255]), it is true that every endomorphism that

takes nonzero linear combinations of generators to primitive elements is an automorphism.

Problem 12.6.9. Let K be an algebraically closed field and φ an endomorphism of a free Lie algebra L of finite rank such that for any nonzero linear combination a of elements of X the image $\varphi(a)$ is a primitive element. Is it true that φ is an automorphism of L?

Problem 12.6.10. Let K be an algebraically closed field and φ either an endomorphism of the polynomial algebra $K[X]$ or of the free associative algebra $K\langle X\rangle$ such that for any nontrivial linear combination h of elements of X the image $\varphi(h)$ is a coordinate polynomial of $K[X]$ (or a primitive element of $K\langle X\rangle$). Is it true that φ is an automorphism?

12.7 Inverse Images of Primitive Elements

Let K be a field and $X = \{x_1, \dots, x_n\}$ a nonempty finite set. In this section, we study combinatorial properties of endomorphisms of free algebras $F(X)$ by considering inverse images of primitive elements.

In this section, $F = F(X)$ is a free K-algebra (without a unit element) on a finite set X of free generators in one of the following varieties of algebras over a field K: the variety of all algebras, the variety of Lie algebras, the variety of Lie p-algebras, varieties of color Lie superalgebras, varieties of color Lie p-superalgebras, or varieties of all nonassociative commutative and anticommutative algebras. We start with inverse images of primitive elements under injective endomorphisms.

Theorem 12.7.1 ([255]). *Let u be an element of a free algebra $F = F(X)$, v a primitive element of F, and φ an injective endomorphism of F such that $\varphi(u) = v$. Then u itself is a primitive element of F.*

Proof. Since v is a primitive element of F, there is a set $Z = \{z_1, \dots, z_n\}$ of free generators of the algebra F such that $v = z_1$.

Let $f_i = \varphi(z_i)$, $1 \le i \le n$. By a finite number of elementary transformations, we transform the set $\{f_1, \dots, f_n\}$ to a reduced (relative to Z) set $\{g_1, \dots, g_n\}$ (since φ is injective, no zeros appear at any step of this procedure). After applying the same sequence of elementary transformations to the set Z of free generators, we get a set $Y = \{y_1, \dots, y_n\}$ of free generators of the algebra F such that $\varphi(y_i) = g_i$, $1 \le i \le n$.

Now we write the element u as $u = u(y_1, \dots, y_n)$. We have

$$\varphi(u) = u(g_1, \dots, g_n) = z_1. \tag{12.9}$$

If $\ell_Z(u) > 1$, then $\ell_Z(\varphi(u)) > 1$, and we arrive at a contradiction with (12.9). Therefore, u is a linear combination of the free generators $z_1, \dots, z_n$. It follows from (12.9) that this linear combination is nonzero. Thus u is a primitive element of the free algebra F. ■

A statement of Theorem 12.7.1 for polynomial algebras in two variables over a field of zero characteristic was proved by L. A. Campbell and J.-T. Yu [65]. For free associative algebras of ranks 2 and 3, it is an open problem. For rank greater than 3, the answer is negative due to V. Shpilrain and J.-T. Yu [367].

Now we consider a more general situation.

Theorem 12.7.2 ([255]). *Let $u_1, \dots, u_k$ be elements of a free algebra $F = F(X)$ of rank n, $\{z_1, \dots, z_k\}$ a primitive system of F, $1 \le k \le n$, and let φ be an injective endomorphism of the algebra F such that $\varphi(u_i) = z_i$, $1 \le i \le k$. Then $\{u_1, \dots, u_k\}$ is a primitive system of the algebra F. Furthermore, if $k = n$, then φ is an automorphism of the algebra F.*

Proof. Complete the system $\{z_1, \dots, z_k\}$ to a free generating set Z of the algebra F by some elements $\{z_{k+1}, \dots, z_n\}$. The same argument as in the proof of Theorem 12.7.1 shows that there is a set $Y = \{y_1, \dots, y_n\}$ of free generators of the algebra F such that

$$\{g_1, \dots, g_n \mid g_i = \varphi(y_i),\ 1 \le i \le n\}$$

is a reduced subset of F relative to the free generating set Z. We write the elements $u_1, \dots, u_k$ in the alphabet Y: $u_i = u_i(y_1, \dots, y_n)$, $1 \le i \le k$. We know that

$$\varphi(u_i) = u_i(g_1, \dots, g_n) = z_i, \quad 1 \le i \le k. \tag{12.10}$$

Therefore

$$u_i = \sum_{j=1}^{n} \alpha_{ij} y_j, \quad \text{where } \alpha_{ij} \in K,\ 1 \le i \le k,$$

and if $\alpha_{ij} \ne 0$ for some i, j, then $\ell_Z(g_j) = 1$ (otherwise, we get a contradiction with (12.10) since the terms of degree > 1 cannot cancel out).

It follows from (12.10) that the elements $u_1, \dots, u_k$ are linearly independent. Thus, $\{u_1, \dots, u_k\}$ is a primitive system of elements of the algebra F, which consists of linear combinations of the free generators $y_1, \dots, y_n$. If $k = n$, then $U = \{u_1, \dots, u_n\}$ is a basis of the vector space generated by the elements $y_1, \dots, y_n$. Hence U is a free generating set of the algebra F, and the endomorphism φ given by $\varphi(u_i) = z_i$, $1 \le i \le n$, is an automorphism of the algebra F. ■

Now we consider inverse images of primitive systems under arbitrary endomorphisms. Recall that a subalgebra H of F is a retract if there exists an ideal I of F such that $F = H \oplus I$.

Theorem 12.7.3 ([255]). *Let $U = \{u_1, \dots, u_l\}$ be a subset of a free algebra $F = F(X)$ of rank $n \ge l$, $\{z_1, \dots, z_l\}$ a primitive system of F, H the subalgebra of F generated by U, and φ an endomorphism of the algebra F*

such that $\varphi(u_i) = z_i$, $1 \leq i \leq l$. *Then* H *is a retract of the algebra* F. *In particular, if* $l = n$, *then* φ *is an automorphism, and* U *is a set of free generators of the algebra* F.

Proof. In view of Theorem 12.7.2, we may assume that φ is not injective (obviously, a primitive system generates a retract).

Complete the set $\{z_1, \ldots, z_l\}$ to a set Z of free generators of the algebra F by some elements $\{z_{l+1}, \ldots, z_n\}$, and let $f_i = \varphi(z_i)$, $1 \leq i \leq n$. By a finite number of elementary transformations, one can transform the set $\{f_1, \ldots, f_n\}$ into a set $\{g_1, \ldots, g_n\}$ such that for some k, $1 \leq k \leq n$, the set $\{g_1, \ldots, g_k\}$ is reduced relative to the alphabet Z, and $g_i = 0$ for $i > k$ (since φ is not injective, we have $k < n$). This sequence of elementary transformations gives rise to an automorphism ψ of the algebra F such that $\psi(x_i) = y_i$, $\varphi(y_i) = g_i$, $1 \leq i \leq n$.

Now we write the elements $u_1, \ldots, u_l$ in the following form:

$$u_i(y_1, \ldots, y_n) = u_i^{(1)}(y_1, \ldots, y_k) + u_i^{(2)}, \quad 1 \leq i \leq l,$$

where for each $i = 1, \ldots, l$ the element $u_i^{(1)}$ depends only on the free generators $y_1, \ldots, y_k$, and the element $u_i^{(2)}$ belongs to the ideal of the algebra F generated by the free generators $y_{k+1}, \ldots, y_n$. We know that

$$\varphi(u_i) = u_i(g_1, \ldots, g_n) = u_i^{(1)}(g_1, \ldots, g_k) = z_i, \quad 1 \leq i \leq l.$$

It follows that

$$u_i^{(1)} = \sum_{j=1}^{k} \alpha_{ij} y_j,$$

where $\ell_Z(g_j) = 1$ whenever $\alpha_{ij} \neq 0$. Hence $l \leq k$.

Let ψ be a linear automorphism of the algebra F such that $\psi(y_i) = u_i^{(1)}$ for $1 \leq i \leq l$, and $\psi(y_j) = y_j$ for $l < j \leq n$. Denote $y_i' = \psi(y_i)$, $1 \leq i \leq n$. Let J be an ideal of the algebra F generated by the free generators y_j' with $l < j \leq n$. It is clear that $u_i = y_i' \pmod{J}$, $1 \leq i \leq l$. Thus, $F = H \oplus J$, whence H is a retract of the algebra F. ■

For a description of retracts of free algebras F, see Section 13.2 in Chapter 13.

13

Generalized Primitive Elements

Let K be a field, $\operatorname{char} K \neq 2$, and let X be a finite set, $X = \{x_1, \ldots, x_n\}$. In what follows, $F = F(X)$ denotes the free K-algebra without the unity element on the set X of free generators of one of the following varieties of algebras over a field K: the variety of all algebras, the variety of Lie algebras, varieties of color Lie superalgebras, the variety of Lie p-algebras, varieties of color Lie p-superalgebras, and varieties of commutative and anticommutative algebras.

Fixed points of endomorphisms and automorphisms of algebraic systems are under intensive consideration by many algebraists. An element u is called a test element if for any endomorphism φ it follows from $\varphi(u) = u$ that φ is an automorphism. This definition was explicitly given by V. Shpilrain in [352]. But the history of test elements goes back to J. Nielsen and W. Dicks. A classical result of Nielsen [293] states that an endomorphism $x \to f$; $y \to g$ of the free group F_2 with two generators x, y is an automorphism if and only if $[f, g]$ is conjugate to $[x, y]$. Hence the commutator $[x, y] = xyx^{-1}y^{-1}$ is a test element of F_2. W. Dicks [93, 94] proved a similar result for the free associative algebra $K\langle x, y\rangle$ of rank 2. In articles [110, 124, 128], test elements of polynomial algebras and of free associative algebras are under consideration.

Test elements of free groups have been of interest for many years. Examples of such elements were given in [82, 100, 115, 131, 132, 147, 151, 165, 293, 314, 316, 317, 318, 319, 320, 321, 352, 355, 383, 417, 418]. In [383], E. C. Turner proved that test elements for monomorphisms of free groups of finite rank are exactly the elements with maximal rank (an element of the free group has maximal rank if it does not belong to any free factor

of the group) and that test elements for endomorphisms of free groups are elements not contained in proper retracts; see our Section 2.2. The analogs of these results for free Lie algebras and free color Lie superalgebras and p-superalgebras were proved by A. A. Mikhalev and A. A. Zolotykh in [277] and by A. A. Mikhalev and J.-T. Yu in [263], respectively. For free ((anti)commutative) nonassociative algebras, these results were obtained by A. A. Mikhalev, U. U. Umirbaev, and J.-T. Yu in [259].

A subalgebra H of F is called a retract if there is a homomorphism $\rho\colon F \to H$ such that ρ is the identity mapping on H (ρ is the retraction homomorphism). Obviously, a subalgebra H of F is a retract if and only if there exists an ideal I of F such that $F = H \oplus I$.

Let F_n be the free group of rank n, h a nonidentity element of F_n, and $\mathrm{Orb}(h)$ the orbit of h under the action of the automorphism group of F_n. The following problem was raised by V. Shpilrain.

Problem 13.0.1 ([352]). Suppose that φ is an endomorphism of F_n such that

$$\varphi(\mathrm{Orb}(h)) \subseteq \mathrm{Orb}(h)$$

for some nonidentity element h of F_n. Is then φ an automorphism of F_n?

For $n = 2$, the positive solution was given by S. V. Ivanov in [154] and by V. Shpilrain in [356]. For an arbitrary n, the problem was settled by D. Lee [206]; see also Theorem 4.3.1. It is interesting to consider the same problem for free algebras (Lie, associative, relatively free algebras). V. Drensky and J.-T. Yu in [109] solved this problem for $n = 2$ for free Lie algebras and for free metabelian associative and Lie algebras. One may consider a special case when h is a primitive element; i.e., h belongs to a free generating set of the free group (or of the free algebra). In [269, 271], A. A. Mikhalev and A. A. Zolotykh solved the problem for free Lie algebras and for free color Lie (p-) superalgebras assuming that h is a primitive element. A. van den Essen and V. Shpilrain in [124] obtained an analogous result for a primitive element h of the polynomial algebra in two variables (of the free associative algebra of rank 2), and they proved that if the Jacobian conjecture (that is, that any endomorphism of the polynomial algebra over a field of characteristic zero with the invertible Jacobian matrix is an automorphism) is true, then the problem has an affirmative answer for a primitive element of the finitely generated polynomial algebra over an algebraically closed field of characteristic zero. Finally, Z. Jelonek [161] proved this statement for polynomial algebras over the field of complex numbers (his proof used methods of algebraic geometry). In [268, 271] A. A. Mikhalev, J.-T. Yu, and A. A. Zolotykh showed that if K is a nonalgebraically closed field, then it is not enough to consider only images of nonsingular linear combinations of free generators. S. V. Ivanov in [154] solved Problem 13.0.1 (under some additional conditions) for a primitive element h of F_n. We have exposed exact solutions of Problem 13.0.1

for primitive elements of free algebras of Schreier varieties of algebras in Section 12.6 of Chapter 12. In the general situation, positive solutions of the problem were obtained by A. A. Mikhalev and J.-T. Yu [264] and by A. A. Mikhalev, U. U. Umirbaev, and J.-T. Yu [259].

In Section 13.1, we consider test elements of the algebra $F = F(X)$: we prove that test elements for monomorphisms of the algebra F are the elements of the maximal rank (Theorem 13.1.1); test elements for endomorphisms of F are elements that do not belong to any proper retract of F (Theorem 13.1.4). Section 13.2 characterizes retracts of the algebra F (Theorem 13.2.1). In Section 13.3, we solve Problem 13.0.1 for finitely generated free algebras of Schreier varieties of algebras: if an endomorphism φ of the algebra F preserves the automorphic orbit of a nonzero element of F, then actually φ is an automorphism (Theorems 13.3.1–13.3.3).

After that, we study generalized primitive elements of free algebras and their automorphic orbits.

Let $\mathfrak{U}$ be a variety of groups defined by the set of laws $\mathfrak{V}$, F the free group, and let $\mathfrak{V}(F)$ be the verbal subgroup defined by $\mathfrak{V}$. An element g of F is said to be $\mathfrak{U}$-generic if $g \in \mathfrak{V}(F)$ but $g \notin \mathfrak{V}(G)$ for every proper subgroup G of F.

In the articles [82, 100, 131, 132, 225, 319, 352, 374, 375, 417] generic elements of free groups were studied. In particular, series of generic elements of free groups were constructed. In [82] it was shown that for a variety with a solvable word problem there is an algorithm to recognize generic elements.

An almost primitive element (APE) is an element of a free group F that is not primitive in F but is primitive in any proper subgroup of F containing it. APEs of a finitely generated free group are test elements [82]. But there are test elements of free groups that are not generic: the element $x^2[y^2, z]$ is a test word but is not generic [82]. An element $x^2yx^{-1}y^{-1}$ is an APE of the free group $F(x, y)$, but it is not a test element. In general, generic does not imply APE [132]. At the same time, in [132] it was proved that if $\mathfrak{U}$ is a nontrivial variety defined by the set of laws $\mathfrak{V}$ and $w \in \mathfrak{V}(F)$, and w is an APE of F, then w is $\mathfrak{U}$-generic and hence a test element in F. A series of interesting results were obtained for almost primitive elements of free groups in [60, 131, 132, 182, 183, 318, 319, 320, 321]. See Section 3.1 for further discussion.

Section 13.4 deals with almost primitive and test elements of free algebras with the Nielsen–Schreier property. We show that almost primitive elements are elements of maximal rank; see Proposition 13.4.1. If the free algebra F is a free product of its subalgebras A and B, and elements a and b are homogeneous almost primitive elements in algebras A and B, respectively, then the element $a + b$ is an almost primitive element in F; see Proposition 13.4.6. This result gives us a possibility to construct in Theorem 13.4.7 a series of almost primitive elements. We discuss also a connection between properties of elements to be almost primitive and to be test elements.

A vector of Laurent polynomials is called Δ-unimodular if its components generate the augmentation ideal of the whole algebra. V. A. Artamonov [20] proved that the general linear group acts transitively on the set of all Δ-primitive vectors (for unimodular vectors, this result was proved by A. A. Suslin [378]). V. Shpilrain [356] considered Δ-primitive elements of the free group. He proved that in a free group F_{2m} any Δ-primitive element is an automorphic image of $[x_1, x_2][x_3, x_4] \dots [x_{2m-1}, x_{2m}]$, there are no primitive elements of the group F_n if n is odd, and in a free group F of finite rank, the group $\mathrm{Aut}(F)$ acts transitively on the set of all Δ-primitive elements; see Section 3.1. By Δ we denote the left ideal of the free associative algebra $K\langle X\rangle$ generated by the set X. Following [356], we say that an element u of $L(X)$ is a Δ-primitive element if the elements $\frac{\partial}{\partial x_1}u, \dots, \frac{\partial}{\partial x_n}u$ generate Δ as the left ideal of $K\langle X\rangle$.

In Section 13.5, we prove Theorem 13.5.1: if the rank n of the free Lie algebra L is even, $n = 2m$, then any Δ-primitive element of L is an automorphic image of $[x_1, x_2] + \dots + [x_{2m-1}, x_{2m}]$, there are no Δ-primitive elements of L if n is odd, and the group of automorphisms of the algebra L acts transitively on the set of all Δ-primitive elements.

In Section 13.6, we consider generic elements of free Lie algebras. Let $\mathfrak{U}$ be a variety of Lie algebras over a field K defined by the set of identities $\mathfrak{V}$, $L = L(X)$ the free Lie algebra with the set X of free generators, and let $\mathfrak{V}(L)$ be the verbal ideal of L defined by $\mathfrak{V}$. An element f of L is said to be $\mathfrak{U}$-generic if $f \in \mathfrak{V}(L)$ but $f \notin \mathfrak{V}(H)$ for every proper subalgebra H of L. Let $\mathfrak{A}$ be the variety of abelian Lie algebras. An element u of the free Lie algebra L is $\mathfrak{A}$-generic if $u \in [L, L]$, and if $u \in [H, H]$ for some subalgebra H of L, then $H = L$. As in the situation with free groups (see [82]), since free Lie algebras of finite rank are Hopfian, generic elements are test elements. Propositions 13.6.1 and 13.6.3 give new examples of almost primitive elements of free Lie algebras. In Proposition 13.6.4 and Theorem 13.6.5, we construct series of examples of $\mathfrak{A}$-generic elements of free Lie algebras. Theorem 13.6.7 gives an example of an $\mathfrak{A}$-generic element of the free Lie algebra $L(x, y)$ that is not an APE of this algebra. In Theorem 13.6.8, we show that the element $u = [x_1, \dots, x_n]$ is an $\mathfrak{N}_n$-generic element of the free Lie algebra $L(X)$, where $\mathfrak{N}_n$ is the variety of nilpotent Lie algebras of degree not less than n.

In this chapter, we propose a series of interesting open problems for future research, Problems 10.3.2, 13.1.5, 13.2.2, 13.3.4, 13.4.8, and 13.6.9.

13.1 Test Elements

In this section, we characterize test elements for monomorphisms (injective endomorphisms) and for endomorphisms of free algebras $F(X)$ of finite rank.

Theorem 13.1.1 ([264]). *Let K be a field, $X = \{x_1, \dots, x_n\}$, $u \in F = F(X)$, $\operatorname{rank}(u) = n$, and φ a monomorphism of F such that $\varphi(u) = u$. Then φ is an automorphism of F.*

Proof. Let $u = u_X^\circ + u_X^*$, where u_X° is the leading component of u relative to the degree in the alphabet X. Let also $u_X^* = u_X^{*\circ} + u_X^{**}$, $u_X^{**} = u_X^{**\circ} + u_X^{***}$, and so on.

For any set Y of free generators of the algebra F, we consider the infinite row

$$Y(u) = (\ell_Y(u), \operatorname{rank}(u_Y^\circ), \ell_Y(u_Y^*), \operatorname{rank}(u_Y^{*\circ}), \dots).$$

We compare such rows lexicographically starting from the left side.

Changing if it is necessary the set X of free generators, one can assume that X has the following minimal property:

$$X(u) = \min_{Y \in \Omega} Y(u),$$

where $\Omega = \{Y \mid Y \text{ is a set of free generators of } F\}$.

Let $h_i = \varphi(x_i)$, $i = 1, \dots, n$, and let $H = \{h_1, \dots, h_n\}$ and B be the subalgebra of F generated by H. Since φ is a monomorphism of F, H is an independent subset of F. There exists a sequence of elementary transformations R such that $R(H) = V = \{v_1, \dots, v_n\}$, $v_i \neq 0$ for all $i = 1, \dots, n$, V is a reduced subset, and V generates the subalgebra B.

Let $Y = \{y_1, \dots, y_n\} = R(X)$. It is clear that Y is a set of free generators of F, $v_i = \varphi(y_i)$ for $1 \leq i \leq n$.

Let $\tilde{u}$ be the presentation of u in generators from Y. Then, using the assumptions of the theorem, we get

$$u(x_1, \dots, x_n) = \tilde{u}(y_1, \dots, y_n) = \tilde{u}(v_1, \dots, v_n), \tag{13.1}$$

where $\tilde{u}(v_1, \dots, v_n)$ is obtained from $\tilde{u}(y_1, \dots, y_n)$ by changing y_i on v_i, $i = 1, \dots, n$.

On the contrary, assume that φ is not an automorphism of F. Since V is a reduced set, it means that $\ell_X(v_j) > 1$ for some j. Without loss of generality, we may suppose that $v_1 = x_1, \dots, v_r = x_r$, $r < n$, and $\ell_X(v_j) > 1$ for all $j = r+1, \dots, n$ (possibly $r = 0$ and $\ell_X(v_i) > 1$ for all i).

It follows from (13.1) that $u(x_1, \dots, x_n) \in B$. Consider now the leading part of the element u:

$$u(x_1, \dots, x_n) = u_X^\circ + u_X^*,$$
$$u_X^\circ = u_X^{\circ 1}(x_1, \dots, x_r) + u_X^{\circ 2},$$

where $u_X^{\circ 1}$ is the component of u_X° that does not depend on generators $x_{r+1}, \dots, x_n$.

If $u_X^{\circ 1} = 0$, then we rewrite u as an element of the subalgebra B with the set V of free generators. Since V is a reduced subset,

$$\ell_V(u(x_1, \dots, x_n)) < \ell_X(u(x_1, \dots, x_n)).$$

Taking into account (13.1), we get

$$\ell_Y(\tilde{u}(y_1,\dots,y_n)) < \ell_X(u(x_1,\dots,x_n)).$$

This gives a contradiction with the minimal property of X relative to u.

In the case where $u_X^{\circ 1} \neq 0$ we have

$$u(x_1,\dots,x_n) = \tilde{u}(v_1,\dots,v_n) = \tilde{u}_V^{\circ} + \tilde{u}_V^{*},$$

where

$$\tilde{u}_V^{\circ} = \tilde{u}_V^{\circ 1}(v_1,\dots,v_r) + \tilde{u}_V^{\circ 2}(v_1,\dots,v_n),$$

and $\tilde{u}_V^{\circ 1}$ is the component of $\tilde{u}_V^{\circ}$ that does not depend on $v_{r+1},\dots,v_n$.

It is evident that

$$\tilde{u}_V^{\circ 1}(v_1,\dots,v_r) = u_X^{\circ 1}(x_1,\dots,x_r).$$

If $\tilde{u}_V^{\circ 2} \neq 0$, then bearing in mind that V is a reduced subset, we obtain

$$\ell_X(\tilde{u}(v_1,\dots,v_r)) > \ell_X(u).$$

It gives a contradiction with (13.1).

Therefore

$$\tilde{u}_V^{\circ} = u_X^{\circ 1}(x_1,\dots,x_r) = u_X^{\circ 1}(v_1,\dots,v_r). \tag{13.2}$$

Now we consider the component $u_X^{\circ 2}$. If $u_X^{\circ 2} \neq 0$, then it follows from (13.2) that

$$\operatorname{rank}(\tilde{u}_Y^{\circ}) = \operatorname{rank}_B(\tilde{u}_V^{\circ}) = \operatorname{rank}(u_X^{\circ 1}) < \operatorname{rank}(u(x_1,\dots,x_n)).$$

As above, it gives a contradiction with the minimal property of X. Hence u_X° does not depend on $x_{r+1},\dots,x_n$. Since $v_1 = x_1,\dots,v_r = x_r$ (i.e., $u_X^{\circ} = u_V^{\circ}$), by analogy we see that the elements $u_X^{*\circ}, u_X^{**\circ},\dots$ do not depend on $x_{r+1},\dots,x_n$.

Thus, the element u does not depend on $x_{r+1},\dots,x_n$, and we have come to a contradiction with the condition $\operatorname{rank}(u) = n$. ■

As a corollary, we have the following theorem:

Theorem 13.1.2 ([264]). *Let $X = \{x_1,\dots,x_n\}$, $u \in F(X)$, $\operatorname{rank}(u) = n$, and let φ be a monomorphism of the free algebra $F = F(X)$. Then φ is an automorphism of F if and only if the element $\varphi(u)$ belongs to the orbit of u under the action of the automorphism group of F ($\varphi(u) \in \operatorname{Orb}(u)$).*

Proof. If φ is an automorphism of F, then our statement is obvious. Now let $\varphi(u) \in \operatorname{Orb}(u)$. Then there exists an automorphism ψ of F such that $\varphi(u) = \psi(u)$. For the monomorphism $\mu = \varphi\psi^{-1}$ of F and for the element $v = \psi(u)$, we have

$$\mu(v) = \varphi\psi^{-1}(\psi(u)) = \varphi(u) = \psi(u) = v,$$

and $\operatorname{rank}(v) = n$. Applying Theorem 13.1.1, we get that $\varphi\psi^{-1}$ is an automorphism. Thus, φ is also an automorphism of F. ■

Lemma 13.1.3. *Let K be a field,* $\operatorname{char} K \neq 2$, $|X| \geq 2$, *and let u be a homogeneous element of $F(X)$ of maximal rank. Then u is a test element.*

Proof. Let φ be an endomorphism of $F(X)$, $h_i = \varphi(x_i)$, $1 \leq i \leq n$. Since $|X| \geq 2$ and u is a homogeneous element of maximal rank, $\ell(u) \geq 2$. It follows now from $\varphi(u) = u$ that elements h_i, $1 \leq i \leq n$, are nonzero, and their component of minimal degree $\bar{h}_i$ has the length 1. Since u is an element of maximal rank, elements $\bar{h}_i$, $1 \leq i \leq n$, are linearly independent. Hence φ is a monomorphism of $F(X)$. Since u is an element of maximal rank, it follows from Theorem 13.1.1 that φ is an automorphism of $F(X)$. ■

Note that the statement of Lemma 13.1.3 for free Lie algebras was proved by V. Shpilrain in [354]. Theorems 13.1.1 and 13.1.2 for free color Lie (p-)superalgebras were obtained by A. A. Mikhalev and A. A. Zolotykh [277].

The statement of Theorem 13.1.1 is not true in general for elements u with $\operatorname{rank}(u) < n$. Indeed, if u does not depend on x_1, then one can consider the endomorphism φ given by $\varphi(x_1) = x_1 \cdot x_2$ and $\varphi(x_i) = x_i$ for any $i > 1$. At the same time, it is impossible to omit the condition that φ is a monomorphism. Indeed, let $X = \{x_1, x_2\}$, $u = x_1 + x_1 \cdot x_2$, $\varphi(x_1) = u$, and $\varphi(x_2) = 0$. Then $\operatorname{rank}(u) = 2 = |X|$, $\varphi(u) = u$, but φ is not an automorphism of $F(X)$. The reason for this fact is that if U is the subalgebra of $F(X)$ generated by the element u and J the ideal of $F(X)$ generated by x_2, then $F(X) = U \oplus J$; that is, the element u belongs to the proper retract U of $F(X)$.

Theorem 13.1.4 ([263, 264]). *Let $X = \{x_1, \ldots, x_n\}$. Test elements of the free algebra $F{=}F(X)$ are precisely those elements not contained in any proper retract of F.*

Proof. Let φ be a nontrivial endomorphism of the algebra F such that φ is not an automorphism of F, $0 \neq u \in F$, and $\varphi(u) = u$.

If φ is a monomorphism of F, then, by Theorem 13.1.1, $\operatorname{rank}(u) < n$; i.e., the element u belongs to a proper free factor of F that is a proper retract of F. Suppose now that φ is not a monomorphism. Let

$$\varphi^{\infty}(F) = \bigcap_{i=0}^{\infty} \varphi^i(F).$$

Since $u \neq 0$, $\varphi^{\infty}(F) \neq 0$, we may suppose that there exists a free generating set Y of F such that for some s, $1 \leq s < n$, we have

$$\varphi(y_i) = u_i \neq 0, \quad 1 \leq i \leq s,$$

and

$$\varphi(y_j) = 0 \quad \text{for} \quad s < j \leq n,$$

the subset $\{u_1, \ldots, u_s\}$ is reduced modulo the ideal J of F generated by the free generators $y_{s+1}, \ldots, y_n$. Let $u_i = \tilde{u}_i + u_i^*$, $1 \leq i \leq s$, where $\tilde{u}_i$ is the component of u_i that depends only on $y_1, \ldots, y_s$, and $u_i^* \in J$. It is clear that $\tilde{u}_i \neq 0$ for all i, $1 \leq i \leq s$. In the same way, we write down the element u in the form $u = \tilde{u} + u^*$. Again it is obvious that $\tilde{u} = \tilde{u}(y_1, \ldots, y_s) \neq 0$. Since

$$u = \varphi(u) = \varphi(\tilde{u}) + \varphi(u^*) = \varphi(\tilde{u}),$$

we get

$$\tilde{u}^\circ = \widetilde{(\varphi(\tilde{u}))}^\circ;$$

that is,

$$\tilde{u}^\circ(y_1, \ldots, y_s) = \tilde{u}^\circ(\widetilde{u_1, \ldots, u_s})^\circ = \tilde{u}^\circ(\tilde{u}_1^\circ, \ldots, \tilde{u}_s^\circ).$$

We may assume that the component $\tilde{u}^\circ$ depends on generators $y_1, \ldots, y_t$, where $1 \leq t \leq s$. Then we get $\ell(u_i) = \ell(y_i)$, $1 \leq i \leq s$. If $t = s$, then the subalgebra H generated by $u_1, \ldots, u_s$ is a proper retract of F, and $u \in H$. If $t < s$, then we consider the decomposition of the component $\tilde{u}$ into the sum of homogeneous components (relative to the length function)

$$\tilde{u} = \tilde{u}^\circ + \tilde{u}^{\circ\circ} + \ldots, \quad \text{where } \tilde{u}^{\circ\circ} = (u^*)^\circ,$$

and so on. Using the same arguments, we obtain that $\ell(u_j) = \ell(y_j)$ for all j such that $\tilde{u}$ depends on y_j. One can suppose that the element $\tilde{u}$ depends on $y_1, \ldots, y_r$, where $t \leq r \leq s$. Since $\varphi(u^*) = 0$,

$$u = \tilde{u}(y_1, \ldots, y_r) + u^* = \varphi(u) = \tilde{u}(u_1, \ldots, u_r).$$

Therefore the element u belongs to the subalgebra H' generated by the elements $u_1, \ldots, u_r$ ($H' \subseteq H \subseteq F$). Using a nonsingular linear transformation of free generators from Y, we may assume that $u_j = y_j + u_j^*$, where $1 \leq j \leq r$, $u_j^* \in J$. Thus H' is a proper retract of F, $u \in H'$.

We have proved that every element u of F not contained in any proper retract of F is a test element for automorphisms of the algebra F. On the other hand, let H be a proper retract of F, $0 \neq u \in H$, and φ the corresponding retraction homomorphism. Then φ is not an automorphism of F but $\varphi(u) = u$. Namely, u is not a test element. This completes the proof. ■

Problem 13.1.5. Construct an algorithm to recognize test elements of free algebras of Schreier varieties of algebras.

L. P. Comerford [82] proved that there is an algorithm to recognize test elements of free groups.

13.2 Retracts

In this section, we show that retracts of free algebras $F(X)$ of finite rank have the same description as retracts of free groups of finite rank (as for retracts of free groups, see, for example, the monograph [231]). For more information about subalgebras and ideals of free algebras of Schreier varieties of algebras, we refer to the monographs [32, 33, 57, 275, 313].

Theorem 13.2.1 ([57, 264]). *Let K be a field, $X = \{x_1, \ldots, x_n\}$, and H be a nonzero subalgebra of the free algebra $F=F(X)$. Then H is a proper retract of F if and only if there exist a set $Y = \{y_1, \ldots, y_n\}$ of free generators of the algebra F, an integer r, $1 \leq r < n$, and a set $U = \{u_1, \ldots, u_r\}$ of free generators of the algebra H such that*

$$u_i = y_i + u_i^*, \quad 1 \leq i \leq r, \tag{13.3}$$

where the elements u_i^* belong to the ideal of the algebra F generated by the free generators $y_{r+1}, \ldots, y_n$.

Proof. If the subalgebra H has a set (13.3) of free generators, then we consider the homomorphism $\rho\colon F \to H$ given by $\rho(y_i) = u_i$ with $1 \leq i \leq r$, and $\rho(y_j) = 0$ with $r < j \leq n$. It is clear that ρ is a retraction homomorphism, $F = H \oplus I$, where I is the ideal of the algebra F generated by the elements $y_{r+1}, \ldots, y_n$. Thus H is a nontrivial proper retract of F.

Now let H be a nontrivial proper retract of F, $\rho\colon F \to H$ the corresponding retraction homomorphism, and

$$b_i = \rho(x_i), \quad 1 \leq i \leq n.$$

Applying a sequence of elementary transformations to the set $\{b_1, \ldots, b_n\}$, we come to a set of free generators $\{u_1, \ldots, u_r\}$ of the subalgebra H. If $r = n$, then ρ is a monomorphism, and H is not a retract of F. Therefore $r < n$. Applying the same sequence of elementary transformations to the set X, we obtain the set

$$Y = \{y_1, \ldots, y_n\}$$

of free generators of the algebra F such that

$$\rho(y_i) = u_i, \quad 1 \leq i \leq r,$$

and

$$\rho(y_j) = 0, \quad r+1 \leq j \leq n.$$

Without loss of generality, one can assume that the set $\{u_1, \ldots, u_r\}$ is reduced relative to the subset $\{y_1, \ldots, y_r\}$. Hence $\operatorname{Ker}\rho$ is equal to the ideal generated by the subset

$$\{y_j \mid r+1 \leq j \leq n\}.$$

Since ρ is the identity mapping on H,

$$\rho(u_i) = u_i = \rho(y_i) \quad \text{with} \quad 1 \leq i \leq r.$$

Hence

$$u_i = y_i + u_i^* \quad \text{with} \quad 1 \leq i \leq r,$$

where the elements u_i^*, $1 \leq i \leq r$, belong to the ideal of the algebra F generated by the subset $\{y_{r+1}, \ldots, y_n\}$ of Y. This completes the proof. ■

One can try to solve Problem 13.1.5 using Theorems 13.1.4 and 13.2.1. In general, the situation seems to be rather complicated. But for free two-generated algebras with the Nielsen–Schreier property, the situation for constructing an algorithm to determine test elements is much simpler. By the description of retracts of finitely generated algebras with the Nielsen–Schreier property given in Theorem 13.2.1, any proper retract of $F(x, y)$ is generated by one element w. There is a free generating set $\{u, v\}$ of $F(x, y)$ such that $w = u + f$, where each monomial in f depends on v. Using Theorem 13.1.4, one may easily see that test elements of the free Lie algebra $L = L(x, y)$ are nonzero elements of the commutator algebra $[L, L]$, this fact was noted in [109]. For other classes of free algebras with the Nielsen–Schreier property, we have to construct an algorithm to determine generating elements of retracts and an algorithm to determine whether an element belongs to the subalgebra generated by a retract generated by one element.

We illustrate these algorithms for a free Lie p-superalgebra $L = L^p(x, y)$ of rank 2. Any element w that generates a proper retract of L has a form $u + f$, where $L = L(u, v)$ and each monomial of the element f depends on v. Therefore, if a given element a of L has no summands of the degree 1, then it is not an element generating a proper retract. If it has linear summands, then by using an automorphism we may write it in a form $a = x' + g$, where $L = L^p(x', y')$ and all monomials of the element g have degree greater than 1. Now, to determine whether a generates a retract or not, it is enough to determine whether g in the standard presentation has the monomials that do not depend on y' (these monomials are p^t-powers of x, $t \geq 1$). Now suppose that for a given element a we decided that a is not an element that generates a retract, but possibly it belongs to the subalgebra generated by an element b, and b generates a proper retract. We suppose that K is a perfect field given constructively, with an algorithm of extracting p-roots. Then the leading monomial $a^{\circ\prime}$ of a is a p^t-power of a leading monomial $b^{\circ\prime}$ of b. We take the minimal possible such t and write b in the form $b = \alpha b^{\circ\prime} + b^*$, where $\alpha \in K$ and b^* is a linear combination with undetermined coefficients of monomials that are less than $b^{\circ\prime}$ (at first by the usual degree and then lexicographically). Since a belongs to the subalgebra generated by b, $[a, b] = 0$. It gives us a system of linear equa-

tions on coefficients. By solving this system we complete the algorithm. A similar algorithm may be used for free Lie superalgebras and for free Lie p-superalgebras of rank 2. For free Lie superalgebras, we may use the algorithm to extract square roots from even elements; this algorithm was described in monographs [33, 275]. For free nonassociative algebras and for free (anti)commutative nonassociative algebras, the situation is different, and we have no analog of the condition $[a, b] = 0$. Thus, to find the element b, we have to solve some system of algebraic equations.

Problem 13.2.2. Is it true that the intersection of two retracts of the free algebra $F{=}F(X)$ is a retract of this algebra?

For free groups, Problem 13.2.2 was solved in the affirmative by G. Bergman in [47].

13.3 Endomorphisms and Automorphic Orbits

In this section, we prove that an endomorphism preserving the automorphic orbit of a nonzero element of $F(X)$ is an automorphism of this algebra.

Theorem 13.3.1 ([264]). *Let K be a field, $X = \{x_1, \dots, x_n\}$, u be a nonzero element of the algebra $F = F(X)$, $\mathrm{Orb}(u)$ the automorphic orbit of the element u, and φ an endomorphism of F such that $\varphi(\mathrm{Orb}(u)) \subseteq \mathrm{Orb}(u)$. Then φ is a monomorphism of F.*

Proof. It is clear that $\varphi(u) = \mu(u)$ for some automorphism μ of F. Then for the endomorphism $\psi = \mu^{-1}\varphi$ we have $\psi(u) = u$. If the element u does not belong to any proper retract of F, then by Theorem 13.1.4 the endomorphism ψ is an automorphism of F, and therefore φ is an automorphism of F.

Now let H be a proper retract of F, $u \in H$. By Theorem 13.2.1, there is a set $Y = \{y_1, \dots, y_n\}$ of free generators of the algebra $F = F(X)$ such that the subalgebra H is generated by the elements

$$v_i = y_i + h_i, \quad \text{with} \quad 1 \leq i \leq l, \ l < n, \tag{13.4}$$

where for all i the element h_i belongs to the ideal of F generated by the elements $y_{l+1}, \dots, y_n$.

Using a linear transformation of the set Y, one may suppose that the elements h_i do not have linear summands. By $h^{(1)}$ we denote the minimal component (by the length in Y) of the element h. Changing the element h of $\mathrm{Orb}(u)$ and the set Y, one may suppose that the presentation (13.4) is such that the component $h^{(1)}$ depends on the minimal possible number of free generators from Y. We may assume that $h^{(1)}$ depends on y_1. If φ is not an automorphism of F, then there exists an automorphism ψ of F such

that $\varphi(\psi(y_1)) = 0$, and the nonzero elements of the set

$$\{\varphi(\psi(y_j)) \mid j > 1\}$$

form a reduced subset relative to the alphabet Y.

Consider the element $v = \varphi(\psi(u))$ and its minimal component $v^{(1)}$. Since $\varphi(\psi(y_1)) = 0$, either $\ell_Y(v^{(1)}) > \ell_Y(u^{(1)})$ and $v \notin \mathrm{Orb}(u)$, or the component $v^{(1)}$ depends on a number of free generators fewer than l. Bearing in mind that l is the minimal number in (13.4), we get $v \notin \mathrm{Orb}(u)$. This contradiction completes the proof of the theorem. ■

Let K be a field, $\mathrm{char}\, K \neq 2$, and $X = \{x_1, \ldots, x_n\}$ a G-graded set. By L_X we denote the free color Lie superalgebra $L(X)$ in the case where $\mathrm{char}\, K = 0$ and the free color Lie p-superalgebra $L^p(X)$ in the case where $\mathrm{char}\, K = p > 2$.

Theorem 13.3.2 ([264]). *Let K be a field, $\mathrm{char}\, K \neq 2$, $X = \{x_1, \ldots, x_n\}$, and let u be a nonzero element of the algebra $L = L_X$, $\mathrm{Orb}(u)$ the automorphic orbit of the element u, and φ an endomorphism of L such that $\varphi(\mathrm{Orb}(u)) \subseteq \mathrm{Orb}(u)$. Then φ is an automorphism of L.*

Proof. By Theorem 13.3.1, φ is a monomorphism of the algebra L. If $\mathrm{rank}(u) = n$, then by Theorem 13.1.1 φ is an automorphism of L. Suppose now that $\mathrm{rank}(u) = l < n$ and φ is not an automorphism of L. Then by Theorem 12.6.3 there exists a set $Y = \{y_1, \ldots, y_n\}$ of free generators of L such that $\varphi(y_1)$ is not a primitive element of L.

Since $\mathrm{rank}(u) = l$, there exists an automorphism ψ of L such that the element $h = \psi(u)$ depends only on $y_1, \ldots, y_l$, $h = h(y_1, \ldots, y_l)$. Taking into account that $\varphi(\mathrm{Orb}(u)) \subseteq \mathrm{Orb}(u)$, we get that for the element

$$\varphi(h) = h(\varphi(y_1), \ldots, \varphi(y_l))$$

there is an automorphism θ of L such that

$$\theta(\varphi(h)) = h(y_1, \ldots, y_l).$$

Now we consider the following endomorphism ξ of L:

$$\xi(y_i) = \varphi(y_i) \quad \text{with} \quad 1 \leq i \leq l;$$
$$\xi(y_j) = \theta^{-1}(y_j) \quad \text{with} \quad l < j \leq n.$$

Let

$$w = [\ldots[[h(y_1, \ldots, y_l), y_{l+1}], y_{l+2}], \ldots, y_n].$$

Then it is clear that $\mathrm{rank}(w) = n$, and

$$\theta(\xi(w)) = \theta([\ldots[[h(\varphi(y_1), \ldots, \varphi(y_l))], \theta^{-1}(y_{l+1})]\ldots, \theta^{-1}(y_n)])$$
$$= [\ldots[h, y_{l+1}]\ldots, y_n] = w.$$

Since $\mathrm{rank}(w) = n$, by Theorem 13.1.1, $\theta\xi$ is an automorphism of L. Hence ξ itself is an automorphism of the algebra L. But the element $\xi(y_1) = \varphi(y_1)$

is not primitive. This contradiction completes the proof of the theorem. ■

Let A be a finitely generated free algebra of the variety $\mathfrak{M}_0$ (the variety of all algebras), $\mathfrak{M}_1$ (the variety of all commutative algebras, $\operatorname{char} K \neq 2$), or $\mathfrak{M}_2$ (the variety of all anticommutative algebras).

Theorem 13.3.3 ([259]). *Let u be a nonzero element of A, $\operatorname{Orb}(u)$ the automorphic orbit of the element u, and φ an endomorphism of A such that $\varphi(\operatorname{Orb}(u)) \subseteq \operatorname{Orb}(u)$. Then φ is an automorphism of A.*

Proof. The proof can be given along the lines of the proof of Theorem 13.3.2 using Theorem 12.6.2. ■

Problem 13.3.4. Let u be a nonzero element of a free associative algebra $K\langle X\rangle$, $\operatorname{Orb}(u)$ the automorphic orbit of the element u, and φ an endomorphism of $K\langle X\rangle$ such that $\varphi(\operatorname{Orb}(u)) \subseteq \operatorname{Orb}(u)$. Does it follow that φ is an automorphism of $K\langle X\rangle$?

13.4 Almost Primitive and Test Elements

An almost primitive element (APE) of a free algebra F is defined as an element that is not primitive in F but is primitive in any proper subalgebra of F containing it. We consider almost primitive elements of finitely generated free algebras of the main types of Schreier varieties of algebras.

Proposition 13.4.1 ([265]). *Almost primitive elements of a free algebra F are elements of the maximal rank (that is, they do not belong to any proper free factor of F). The reverse statement is not true.*

Proof. Let a be an APE of F and B a proper free factor of F. Then the element a is primitive in B, and thus a is a primitive element of F. If $F = F(x, y)$, a free algebra of rank 2, then the element $(xy)y$ has the maximal rank 2, but at the same time it is not primitive in the subalgebra generated by xy and y. Hence $(xy)y$ is not an APE of F. ■

Since elements of the maximal rank are test elements for injective endomorphisms of F, it is interesting to realize the difference between almost primitive elements and test elements.

Lemma 13.4.2. *Let K be a field, $\operatorname{char} K \neq 2$, and let u be an APE of $F(X)$ whose component of degree 1 is equal to zero. Then u is a test element of $F(X)$.*

Proof. By Theorem 13.1.4, test elements of the algebra $F(X)$ are precisely those elements not contained in any proper retract of $F(X)$. Let H be a proper retract of $F(X)$, $u \in H$. Since u is an APE of $F(X)$, it is a primitive element of H. Since the automorphism group of H is generated

by elementary automorphisms, it follows from Theorem 13.2.1 that u has a nonzero linear component. This contradiction completes the proof. ■

Proposition 13.4.3 ([265]). *Let K be a field,* $\operatorname{char} K \neq 2$.

1. *xy is an APE of $F(x,y)$, and it is also a test element.*
2. *$x+xy$ is an APE of $F(x,y)$, and at the same time it is not a test element; $(xy)z$ is not an APE of $F(x,y,z)$, and at the same time it is an element of maximal rank.*
3. *xx is an APE of the free nonassociative algebra $F(x)$, and it is also a test element; if y is an odd variable, then $[y,y]$ is an APE of the free Lie superalgebra $L(y)$ of rank 1, and it is also a test element.*
4. *x^p is an APE of the free Lie p-algebra $L^p(x)$, and it is also a test element; x^{p^2} is a test element but not an APE.*
5. *The element $x-[[x,y],y]$ is not an APE of the free Lie algebra $L(x,y)$; also it is not a test element, but it has the maximal rank 2; the element $[[x,y],y]$ is not an APE, but it is a test element of $L(x,y)$.*
6. *$[x,y]+[[x,z],z]$ is an APE of the free Lie algebra $L(x,y,z)$, and it is also a test element.*
7. *If x and y are even, and z is odd, then $[z,y]+[[z,x],x]$ is an APE of the free Lie superalgebra $L(x,y;z)$, and it is also a test element; if y and z are even and x is odd, then this element is neither APE nor a test element of $L(y,z;x)$.*
8. *If $\operatorname{char} K = p > 2$, then the element $x+[y,z]+(\operatorname{ad} x)^p(z)$ is an APE and it is not a test element of the free Lie algebra $L(x,y,z)$, and it is not an APE of the free Lie p-superalgebra $L^p(x,y,z)$.*

Proof. Suppose that one of the elements of points 1–8 belongs to a finitely generated subalgebra H of $F(X)$. We denote this element by u. Let $x > y > z$, and let $\{h_1,\dots,h_m\}$ be a reduced set of free generators of H. By Theorem 11.1.1, the leading part u° of u is a polynomial in $h_1^\circ,\dots,h_m^\circ$.

1. $u = xy = u^\circ$. If u° is a linear combination of some of h_i°, $1 \leq i \leq m$, then it is clear that u is a primitive element of H. Otherwise we may suppose that $u^\circ = h_1^\circ h_2^\circ$, $h_1^\circ = x$, $h_2^\circ = y$. Then $H = F(x,y)$, and H is not a proper subalgebra of $F(x,y)$. By Lemma 13.4.2, xy is a test element of $F(x,y)$.

2. To show that $u = x+xy$ is an APE of $F(x,y)$, one may use the same arguments as in point 1 of the proof. Let φ be the homomorphism of $F(x,y)$ given by $\varphi(x) = u$ and $\varphi(y) = 0$. Then φ is not an automorphism, $\varphi(u) = u$, and u is not a test element of $F(x,y)$.

For the element $v = (xy)z$, we set $h_1 = xy$, $h_2 = z$. Let H be the subalgebra of $F(x,y,z)$ generated by h_1 and h_2. It is clear that $\{h_1,h_2\}$ is a reduced set, and H is a proper subalgebra of $F(x,y,z)$. At the same

time, $v = h_1h_2$, and v is not a primitive element of H. It is obvious that v has the maximal rank.

3, 4. To show that xx, x^p, and $[y, y]$ are APE and test elements of $F(x)$, $L^p(x)$, and $L(y)$, respectively, one may use arguments from point 1 of the proof.

Let H be the subalgebra of $L^p(X)$ generated by the element $w = x^p$, and $v = x^{p^2}$. Then H is a proper subalgebra of $L^p(x)$, $v \in H$, $v = u^p$, and v is not a primitive element of H. Thus x^{p^2} is not an APE of $L^p(X)$. At the same time, the algebra $L^p(x)$ has no proper retracts. Hence any nonzero element of $L^p(x)$ is a test element.

5. Let $u = x - [[x, y], y]$, $h_1 = [x, y] - x$, $h_2 = y$, and let H be the subalgebra of $L(x, y)$ generated by $\{h_1, h_2\}$. It is clear that $\{h_1, h_2\}$ is a reduced set, H is a proper subalgebra of $L(x, y)$, and u is not a primitive element of H ($u = -(h_1 + [h_1, h_2])$). Therefore u is not an APE of $L^p(x, y)$. Taking the retraction homomorphism φ given by $\varphi(x) = u$, $\varphi(y) = 0$, we get $\varphi(u) = u$. Thus u is not a test element of $L(x, y)$. At the same time, u is an element of the maximal rank in $L(x, y)$ (otherwise it is a primitive element, which is not the case).

It is clear that $v = [[x, y], y]$ is not an APE of $L(x, y)$, but v is a test element of $L(x, y)$.

6. For $u = [x, y] + [[x, z], z]$, we have $u^\circ = [[x, z], z]$. If u° is a linear combination of some h_i°, then u is a primitive element of H. Otherwise we have to consider the following cases. In the first case $h_1^\circ = [x, z]$, $h_2^\circ = z = h_2$. Then

$$h_1 = [x, z] + \alpha x + \beta y + \gamma z, \quad \alpha, \beta, \gamma \in K,$$

and $u - [h_1, h_2] = [x, y] - \alpha[x, z] - \beta[y, z]$. If now h_3° contains a summand $[x, y]$, then u is a primitive element of H, and if $h_3^\circ = x$, $h_4^\circ = y$, then $\{h_1, h_2, h_3, h_4\}$ is not a reduced set.

In the second case, $h_1^\circ = x = h_1$, $h_2^\circ = z = h_2$. Then

$$u - [[h_1, h_2], h_2] = [x, y].$$

If h_3° has the summand $[x, y]$, then u is a primitive element, and if $h_4 = y$, then H is not a proper subalgebra, $H = L(x, y, z)$.

By Lemma 13.4.2, u is a test element of $L(x, y, z)$.

7. If x and y are even and z is odd, then using the same arguments as in point 6 of the proof, we get that $[z, y] + [[z, x], x]$ is APE and a test element of $L(x, y; z)$.

If y and z are even and x is odd, then $[z, y] + [[z, x], x] = [z, y] + \frac{1}{2}[x, x]$, and it is not an APE of $L(y, z; x)$. To show that it is not a test element, one may consider the retraction homomorphism φ given by $\varphi(x) = 0$, $\varphi(y) = y + \frac{1}{2}[x, x]$, and $\varphi(z) = z$.

8. In Section 12.5.2 of Chapter 12, it was shown that $u = x + [y, z] + (\operatorname{ad} x)^p(z)$ is not a primitive element of $L(x, y, z)$. Let u belong to a proper subalgebra H of $L(x, y, z)$. We have $u^\circ = (\operatorname{ad} x)^p(z)$, and u° is a polynomial

in $h_1^\circ, \ldots, h_m^\circ$. If u° is a summand of h_1°, then obviously u is a primitive element of H. Otherwise, we may suppose that $h_1 = h_1^\circ = x$, $h_2^\circ = (\operatorname{ad} x)^s(z)$, $s < p$. Let $h_2 = h_2^\circ + h_2^*$. Consider the following element:

$$u' = u - h_1 - (\operatorname{ad} h_1)^{p-s}(h_2) = [y, z] - (\operatorname{ad} h_1)^{p-s}(h_2).$$

Then to write u as an element of H in free generators h_i, we consider u', u'', and so on. At some step of this expression, we get either that $[y, z]$ is a summand (up to a nonzero coefficient) of some h_i° (and then u has the form $\alpha g_i + f(g_j \mid j \neq i)$, $0 \neq \alpha \in K$, and u is a primitive element of H), or $h_j = y$, $h_{j+1} = z$ for some j, and H is not a proper subalgebra of $L(x, y, z)$.

Now we consider the retraction homomorphism φ given by $\varphi(x) = u$ and $\varphi(y) = \varphi(z) = 0$. Then $\varphi(u) = u$, and φ is not an automorphism of $L(x, y, z)$. Hence u is not a test element.

It remains to show that u is not an APE of $L^p(x, y, z)$. Indeed, u is a primitive element of $L^p(x, y, z)$, and $u = x + [y + x^p, z]$. It completes the proof of the proposition. ■

Lemma 13.4.4 ([265]). *Let $F(X)$ be a free product of two of its proper subalgebras, $F = A * B$. Let also a be an APE of A and b an APE of B. Then $a + b$ is not a primitive element of F.*

Proof. Let $Y = \{y_1, \ldots, y_s\}$, $Z = \{z_1, \ldots, z_t\}$, $s+t = n = |X|$, $A = F(Y)$, $B = F(Z)$, $X = Y \cup Z$. Suppose to the contrary that $a + b$ is a primitive element of $F(X)$. Since a and b are APE of A and B, respectively, $l_Y(a) > 1$ and $l_Z(b) > 1$.

Let $G = \{g_1, \ldots, g_n\}$ be a free generating set of $F(X)$, $g_1 = a + b$. Let g_i', $1 \leq i \leq n$, be the component of g_i that does not depend on elements from Z. It is clear that $g_1' = a$. Using elementary automorphisms, we may assume that nonzero elements of the set $\{g_2', \ldots, g_n'\}$ form a reduced subset of A, $l_Y(g_i') < l_Y(g_1) = l_Y(a)$, $2 \leq i \leq n$. Since G is a free generating set of $F(X)$, by a finite number of elementary automorphisms, we may transform the set $G' = \{g_1', \ldots, g_n'\}$ to the free generating set Y of A (join with some zero elements). Let φ be the composition of these elementary automorphisms. If $\varphi(g_1') \neq 0$, then a is a primitive element of A, which gives us a contradiction with the fact that a is an APE of A.

If $\varphi(g_1') = 0$, then each monomial of $\varphi(g_1)$ depends on elements of Z. We may assume that $\varphi(g_2)' = y_1, \ldots, \varphi(g_{s+1})' = y_s$. Hence, using additional elementary automorphisms, we may suppose that $\varphi(g_{s+2})' = \cdots = \varphi(g_n)' = 0$. It is clear that the elements $\varphi(g_1), \varphi(g_{s+2}), \ldots, \varphi(g_n)$ generate the algebra B modulo the ideal of F generated by the set Y. By $\varphi(g_i)''$ we denote the component of $\varphi(g_i)$ that does not depend on elements of Y. Then the set

$$H = \{\varphi(g_1)'', \varphi(g_{s+2})'', \ldots, \varphi(g_n)''\}$$

generates the algebra B. But this set consists of t elements. Since the rank of the algebra B is equal to t and (by Theorem 11.1.1) the algebra B is

Hopfian, H is a set of free generators of B. Thus $\varphi(g_1)''$ is a primitive element of B. Applying the invertible automorphism φ^{-1}, we have $b = \varphi^{-1}(\varphi(g_1)'')$. Thus b is a primitive element of B. But b is an APE of B, and we have come to a contradiction. Thus $a+b$ is not a primitive element of $F(X)$. ■

Lemma 13.4.5 ([265]). *Let $F(X)$ be a free product of two of its proper subalgebras A and B, $F = A * B$. Let also a be an APE of A, b an APE of B, and H a proper subalgebra of F such that $a, b \in H$. Then $a+b$ is a primitive element of H.*

Proof. Let $A = F(Y)$, $B = F(Z)$, $Y = \{y_1, \dots, y_s\}$, $Z = \{z_1, \dots, z_t\}$. We may suppose that H is a finitely generated subalgebra. Using Kurosh's method for construction of free generating sets of free subalgebras (see Section 11.1 of Chapter 11), we see that $H = H_1 * H_2 * H_3$, where H_1 is the subalgebra of all elements of H that do not depend on Z, H_2 is the subalgebra of all elements of H that do not depend on Y, and H_3 is some finitely generated subalgebra (possibly $H = H_1 * H_2$). Hence $a \in H_1$ and $b \in H_2$, and H_1 and H_2 are subalgebras of A and B, respectively. Since H is a proper subalgebra of F, $H_1 \neq A$ or $H_2 \neq B$. Without loss of generality, we may suppose that H_1 is a proper subalgebra of A. Since a is an APE of F and $a \in H_1$, a is a primitive element of H_1. Hence $a+b$ is a primitive element of F. ■

Consider a generalized degree function $\mu\colon X \to \mathbb{N}$, where $\mathbb{N}$ is the set of positive integers. Let $\Gamma(X)$ be the free groupoid of nonassociative monomials in the alphabet X, $S(X)$ the free semigroup of associative words in X, and $^\sim\colon \Gamma(X) \to S(X)$ the bracket removing homomorphism. We set $\mu(x_1 \dots x_n) = \sum_{i=1}^n \mu(x_i)$ for $x_1, \dots, x_n \in X$. If $\mu(x) = 1$ for all $x \in X$, then μ is just the usual length, $\mu = \ell = \ell_X$. If $a \in F(X)$, $a = \sum \alpha_i a_i$, $0 \neq \alpha_i \in K$, a_i are basic monomials, and $a_j \neq a_s$ with $j \neq s$, then we set $\mu(a) = \max_i\{\mu(\tilde{a}_i)\}$. By $\hat{a}$ we denote the leading part of a: $\hat{a} = \sum_{j,\mu(a_j)=\mu(a)} \alpha_j a_j$. To separate cases where we use the length function, we denote the leading part of an element a with respect to the usual degree function by a°.

Proposition 13.4.6 ([265]). *Let $F(X)$ be a free product of two of its proper subalgebras A and B, $F = A * B$. Let also a and b be homogeneous APEs of A and B relative to some generalized degree functions μ_1 and μ_2 of A and B, respectively (μ_1 and μ_2 could be different). Then $a+b$ is an APE of F.*

Proof. By Lemma 13.4.4, $a+b$ is not a primitive element of $F(X)$. Let H be a proper finitely generated subalgebra of F, and let $a+b \in H$. If $a \in H$, then $b \in H$, and by Lemma 13.4.5, $a+b$ is an APE in F. If $a \notin H$, then we consider the generalized degree function μ where restrictions on A and B are equal to μ_1 and μ_2, respectively. Let G be a reduced set of free

generators of H (relative to μ). Without loss of generality, we may assume that the leading μ-component of $a+b$ is equal to a. By H' we denote the subalgebra of $F(X)$ generated by H and the element a. Then $H' \neq F(X)$ (by Kurosh's method, we may construct such a set V of free generators of H' that $a \in V$). By Lemma 13.4.5, $a+b$ is a primitive element of H'. Therefore, by Proposition 11.4.3, $a+b$ is a primitive element of H. Thus $a+b$ is an APE of $F(X)$. ■

Note that if a free group F of finite rank is a product of two of its proper subgroups A and B, $F = A * B$, and a and b are APEs of A and B, respectively, then ab is an APE of F; see [60, 131, 132, 319].

Theorem 13.4.7 ([265]). *Let K be a field with* $\operatorname{char} K \neq 2$.

1. *If $n = 2m$, then the element*
$$x_1x_2 + x_3x_4 + \cdots + x_{2m-1}x_{2m}$$
is an APE of $F(X)$.
2. *If $n = 2m+1$, then the element*
$$x_1x_2 + x_3x_4 + \cdots + x_{2m-1}x_{2m} + x_{2m+1}x_{2m+1}$$
is an APE of the free nonassociative algebra $F(X)$; the element
$$[x_1, x_2] + [x_3, x_4] + \cdots + [x_{2m-1}, x_{2m}] + x_{2m+1}^p$$
is an APE of the free Lie p-algebra $L^p(X)$.
3. *The element $x_1^p + \cdots + x_n^p$ is an APE of the free Lie p-algebra $L^p(X)$.*
4. *If $n = 2m+1$ and $X = \{x_1, \ldots, x_{2m+1}\}$, then the element*
$$[[x_2, x_1], x_1] + [x_2, x_3] + \cdots + [x_{2m}, x_{2m+1}]$$
is an APE element of the free Lie algebra $L(X)$.
5. *Let $X = \{x_1, \ldots, x_n\}$ be even variables and $Y = \{y_1, \ldots, y_m\}$ odd variables.*
   (a) *If $n = 2k$ and $m = 2l$, then the element*
   $$[x_1, x_2] + \cdots + [x_{2k-1}, x_{2k}] + [y_1, y_2] + \cdots + [y_{2l-1}, y_{2l}]$$
   is an APE of the free Lie superalgebra $L(X;Y)$ and of the free Lie p-superalgebra $L^p(X;Y)$.
   (b) *If $n = 2k+1$ and $m = 2l$, then the element*
   $$[[x_2, x_1], x_1] + [x_2, x_3] + \cdots + [x_{2k}, x_{2k+1}] + [y_1, y_2] + \cdots + [y_{2l-1}, y_{2l}]$$
   is an APE of the free Lie superalgebra $L(X;Y)$.
   (c) *If $n = 2k$ and $m = 2l+1$, then the element*
   $$[y_{2l+1}, x_{2k-1}] + [[y_{2l+1}, x_{2k}], x_{2k}] + [x_1, x_2] + \ldots + [x_{2k-3}, x_{2k-2}] + [y_1, y_2] + \cdots + [y_{2l-1}, y_{2l}]$$

is an APE of the free Lie superalgebra $L(X;Y)$.

(d) $x_1^p + \cdots + x_n^p + [y_1, y_1] + \cdots + [y_m, y_m]$ *is an APE of the free Lie p-superalgebra* $L^p(X;Y)$.

(e) *If* $n = 2k+1$ *and* $m = 2l$, *then the element*

$$[x_1, x_2] + \cdots + [x_{2k-1}, x_{2k}] + x_{2k+1}^p + [y_1, y_2] + \cdots + [y_{2l-1}, y_{2l}]$$

is an APE of the free Lie p-superalgebra $L^p(X;Y)$.

(f) *If* $n = 2k$ *and* $m = 2l+1$, *then the element*

$$[x_1, x_2] + \cdots + [x_{2k-1}, x_{2k}] + [y_1, y_2] + \cdots + [y_{2l-1}, y_{2l}] + [y_{2l+1}, y_{2l+1}]$$

is an APE of the free Lie superalgebra $L(X;Y)$ *and of the free Lie p-superalgebra* $L^p(X;Y)$.

(g) *If* $n = 2k+1$ *and* $m = 2l+1$, *then the element*

$$[x_1, x_2] + [x_3, x_4] + \cdots + [x_{2k-1}, x_{2k}] + x_{2k+1}^p + [y_1, y_2] + \cdots + [y_{2l-1}, y_{2l}] + [y_{2l+1}, y_{2l+1}]$$

is an APE of the free Lie p-superalgebra $L^p(X;Y)$.

All elements pointed out above are test elements of the corresponding free algebras.

Proof. The elements xx, $x_i x_j$, x^p are homogeneous relative to the usual degree, and the element $[x, y] + [[x, z], z]$ is μ-homogeneous for μ given by $\mu(x) = \mu(y) = 2$ and $\mu(z) = 1$. Applying Propositions 13.4.3 and 13.4.6, we get that described elements are APEs of $F(X)$. By Lemma 13.4.2, these elements are test elements of $F(X)$. ■

Problem 13.4.8. Find an algorithm to recognize the APE of free algebras of Schreier varieties.

Test elements in free associative algebras are considered in our Section 10.2.

13.5 Δ-Primitive Elements of Free Lie Algebras

In this section, we obtain a characterization of Δ-primitive elements of free Lie algebras. We prove that in free Lie algebras of odd rank there are no such elements, and in free Lie algebras of even rank all these elements are automorphic images of one particular element.

By Δ we denote the left ideal of the free associative algebra $K\langle X\rangle$ generated by the set X. Following [356], we say that an element u of the free Lie algebra $L(X)$ is called a Δ-primitive element if the elements $\frac{\partial}{\partial x_1}u, \ldots, \frac{\partial}{\partial x_n}u$ generate Δ as the left ideal of $K\langle X\rangle$.

Theorem 13.5.1 ([265]). *Let* K *be a field,* $\operatorname{char} K \neq 2$, *and* $X = \{x_1, \ldots, x_n\}$. *Let also* $L(X)$ *be the free Lie algebra on* X *over* K. *Then:*

1. *If $n = 2m$, then any Δ-primitive element is an automorphic image of*

$$[x_1, x_2] + [x_3, x_4] + \cdots + [x_{2m-1}, x_{2m}].$$

2. *There are no Δ-primitive elements of $L(X)$ if n is odd.*

3. *The automorphism group of the algebra $L(X)$ acts transitively on the set of all Δ-primitive elements.*

Proof. Let $X = \{x_1, \ldots, x_n\}$. Recall that an additive function $\omega\colon \mathbb{Z}_+^n \to \mathbb{Q}_+$ is a functional if $\omega(r) \neq 0$ for all $r \neq 0$ (here $\mathbb{Z}_+$ is the set of all nonnegative integers, and $\mathbb{Q}_+$ is the set of all nonnegative rational numbers).

It is clear that an automorphic image of a Δ-primitive element is again a Δ-primitive element. Let $\omega_i = \omega(x_i)$, $1 \leq i \leq n$. We consider a partial ordering on rows $\Omega = (\omega_1 \ldots, \omega_n)$: we say that $\Omega' > \Omega$ if $\omega_i' \geq \omega_i$, $1 \leq i \leq n$, and $\omega_j' > \omega_j$ for some j. Now let ω be a functional with the maximal row Ω such that the leading component $\hat{v}$ with respect to ω of some automorphic image v of the element u has the degree 1 (now we generalize the degree function using the degree ω_i of free generators x_i). We may suppose that $u = v$.

It is clear that the element u has no summands of the length one (that is, the linear combinations of elements of X). Since u is a Δ-primitive element, it has the maximal rank and depends on $x_1, \ldots, x_n$, and there are elements $m_{ij} \in K\langle X\rangle$, $1 \leq i, j \leq n$, such that

$$m_{i1}\frac{\partial u}{\partial x_1} + \cdots + m_{in}\frac{\partial u}{\partial x_n} = x_i, \quad i = 1, \ldots, n. \tag{13.5}$$

Suppose that the length (the usual degree) of the element u is greater than 2. Then it follows from (13.5) that for the leading component $\hat{u}$ of the element u (which has ω-degree equal to 1) there is a relation

$$m_1\frac{\partial \hat{u}}{\partial x_1} + \cdots + m_n\frac{\partial \hat{u}}{\partial x_n} = 0,$$

with not all elements m_i of $K\langle X\rangle$, $1 \leq i \leq n$ equal to zero. Then there is an ω-homogeneous automorphism φ of $L(X)$ (that is, $\omega(\varphi(x_i)) = \omega(x_i)$ for all i) such that the leading component v° of the element $v = \varphi(x_i)$ depends on less than n free generators from X. We may assume that $\hat{v}$ does not depend on x_1. Since v depends on x_1, we may consider the following functional ω'. We increase the rational number $\omega_1 = \omega(x_1)$ until the moment when the leading component of v relative to the new functional depends on x_1. We fix this value for ω_1', and we set $\omega_i' = \omega_i$ for $i = 2, \ldots, n$. Then the leading component of the element v relative to ω' has the ω'-weight equal to 1. At the same time, $\Omega' > \Omega$ by the first component, and we have come to a contradiction with the maximal property

of the functional ω. Thus the length of the element u is equal to 2, and

$$u = \sum_{1 \le i < j \le n} \alpha_{ij}[x_i, x_j], \quad \alpha_{ij} \in K,$$

with not all zero coefficients α_{ij}. Since u has the maximal rank, applying a linear automorphism in new free generators $Y = \{y_1, \dots, y_n\}$, we have

$$u = [y_1, y_2] + \sum_{3 \le i < j \le n} \beta_{ij}[y_i, y_j], \quad \beta_{ij} \in K.$$

Bearing in mind that u is an element of the maximal rank and continuing this process, we get that in the case where $n = 2m$ the initial element u is an automorphic image of

$$[x_1, x_2] + [x_3, x_4] + \cdots + [x_{2m-1}, x_{2m}],$$

which is statement 1 of the theorem. And it is clear now that there are no Δ-primitive elements of $L(X)$ if n is odd (this is statement 2 of the theorem). It follows from statements 1 and 2 that the automorphism group of the algebra $L(X)$ acts transitively on the set of all Δ-primitive elements (which is statement 3). It completes the proof. ■

Corollary 13.5.2. *Let K be a field,* $\operatorname{char} K \neq 2$, *and $X = \{x_1, \dots, x_{2m}\}$. Let also $L(X)$ be the free Lie algebra on X over K. Suppose that φ is an endomorphism of $L(X)$ such that for any Δ-primitive element u of $L(X)$ the element $\varphi(u)$ is also Δ-primitive. Then φ is an automorphism of $L(X)$.*

Proof. Let $w = [x_1, x_2] + \cdots + [x_{2m-1}, x_{2m}]$ and $v = \varphi(w)$. Elements w and v are Δ-primitive. By Theorem 13.5.1, there is an automorphism ψ of $L(X)$ such that $\psi(v) = w$. Therefore $\psi(\varphi(w)) = w$. But w is a test element of $L(X)$. It follows that $\psi\varphi$ is an automorphism. Thus φ is an automorphism of $L(X)$. ■

13.6 Generic Elements of Free Lie Algebras

In this section, we construct a series of generic elements of free Lie algebras and present an example of an almost primitive element that is not generic.

Let $\mathfrak{U}$ be a variety of Lie algebras over a field K defined by the set of identities $\mathfrak{V}$, $L = L(X)$ the free Lie algebra with the set X of free generators, and let $\mathfrak{V}(L)$ be the verbal ideal of L defined by $\mathfrak{V}$. An element f of L is said to be $\mathfrak{U}$-generic if $f \in \mathfrak{V}(L)$ but $f \notin \mathfrak{V}(H)$ for every proper subalgebra H of L. Let $\mathfrak{A}$ be the variety of abelian Lie algebras. An element u of the free Lie algebra L is $\mathfrak{A}$-generic if $u \in [L, L]$, and if $u \in [H, H]$ for some subalgebra H of L, then $H = L$.

Let X be a finite set. Consider a generalized degree function $\mu\colon X \to \mathbb{N}$, where $\mathbb{N}$ is the set of positive integers. By $\hat{a}$ we denote the leading part

of a. We denote the leading part of an element a with respect to the usual degree function by a°.

As in the situation with free groups (see [82]), since free Lie algebras of finite rank are Hopfian, generic elements are test elements.

For $a \in L(X)$, by $\operatorname{ad} a$ and $\operatorname{Ad} a$ we denote the operators of left and right multiplication, respectively, $(\operatorname{ad} a)(b) = [a, b]$ and $(b)\operatorname{Ad}(a) = [b, a]$ for $b \in L(X)$.

Proposition 13.6.1 ([260]). *Let K be a field, $\operatorname{char} K \neq 2$, and $X = \{x, y, z\}$. Then the element $u = [x, y] + (x)(\operatorname{Ad} z)^k$ $(k \geq 2)$ is an APE of the free Lie algebra $L(X)$ over K. It is also a test element of $L(X)$.*

Proof. Suppose that the element u belongs to a finitely generated subalgebra H of $L(X)$. Let $x > y > z$, and let $\{h_1, \ldots, h_m\}$ be a reduced set of free generators of H. Then the leading part u° of u is a polynomial in $h_1^\circ, \ldots, h_m^\circ$.

It is clear that $u^\circ = (x)(\operatorname{Ad} z)^k$. If in the expression of u° we have a nonzero linear summand h_i° for some i, then $u^\circ = \alpha h_i^\circ + f(\{h_j^\circ \mid j \neq i\})$, $0 \neq \alpha \in K$; therefore $u = \alpha h_i + f'(\{h_j \mid j \neq i\})$, and u is a primitive element of H. Otherwise $z \in H$.

Now we consider the generalized degree function μ given by $\mu(x) = 1$, and $\mu(y) = N > k$, $\mu(z) = 1$. Let $\{h_1', \ldots, h_m'\}$ be a reduced set of free generators of the subalgebra H with respect to μ. We have $\hat{u} = [x, y]$, and $\hat{u}$ is a polynomial in $\widehat{h_1'}, \ldots, \widehat{h_m'}$. If $\hat{u}$ has a nonzero linear summand $\hat{h}_j$ for some j, then

$$\hat{u} = \beta \hat{h}_j + g(\{\hat{h}_i \mid i \neq j\}), \quad 0 \neq \beta \in K;$$

therefore $u = \beta h_j + g'(\{h_i \mid i \neq j\})$, and u is a primitive element of H. Otherwise $x \in H$.

If $x, z \in H$, then $u' = u - (x)(\operatorname{Ad} z)^k = [x, y] \in H$. If $(u')^\circ$ has a linear summand in the expression in $h_1^\circ, \ldots, h_m^\circ$, then u is a primitive element of H. Otherwise $y \in H$, and $H = L(X)$. Thus u is an APE of $L(X)$. Since the component of degree one of u is zero, by Lemma 13.4.2 u is a test element of $L(X)$. ■

Proposition 13.6.2 ([260]). *The element*

$$u = (x)(\operatorname{Ad} y)^k + (x)(\operatorname{Ad} z)^l, \quad \textit{where } k \textit{ and } l \textit{ are positive integers,}$$

is an APE of $L(x, y, z)$ if and only if $\min\{k, l\} = 1$ and $\max\{k, l\} \geq 2$.

Proof. If $k = l = 1$, then $u = [x, y + z]$, and u is not a primitive element of the proper subalgebra of $L(x, y, z)$ generated by x and $y + z$.

Suppose that $k, l > 1$. Let $u_1 = (x)(\operatorname{Ad} y)^{k-1}$, $u_2 = (x)(\operatorname{Ad} z)^{l-1}$, $u_3 = y$, $u_4 = z$. Then $U = \{u_1, u_2, u_3, u_4\}$ is a reduced set, $u = [u_1, u_2] + [u_3, u_4]$, $H = L(u_1, u_2, u_3, u_4) \neq L(x, y, z)$, and u is not a primitive element of H. Hence u is not an APE of $L(x, y, z)$. Using Proposition 13.6.1, we complete the proof. ■

Now we consider elements

$$u_{k,l}(x,y) = (\operatorname{ad} x)^k(y) + (x)(\operatorname{Ad} y)^l$$

of the free Lie algebra $L(x,y)$. If $k = l = 2$, then $u_{2,2}(x,y) = [[x,y], x-y]$, and this element is not an APE of $L(x,y)$. If $\operatorname{char} K = p > 2$, then

$$u_{p,p}(x,y) = [x+y, (\operatorname{ad}^{p-1}(x+y))(y-x)],$$

and $u_{p,p}(x,y)$ is not an APE of $L(x,y)$.

Proposition 13.6.3 ([260]). *If $k,l \geq 2$ and $k \neq l$, then the element*

$$u_{k,l}(x,y) = (\operatorname{ad} x)^k(y) + (x)(\operatorname{Ad} y)^l$$

is an APE of $L(x,y)$.

Proof. We may suppose that $k > l$. In this case, $u^\circ_{k,l}(x,y) = (\operatorname{ad} x)^k(y)$. Suppose that the element u belongs to a finitely generated subalgebra H of $L(X)$. Let $\{h_1, \ldots, h_m\}$ be a reduced set of free generators of H. Then the leading part u° of u is a polynomial in $h_1^\circ, \ldots, h_m^\circ$. As in the proof of Proposition 13.6.1, if u is not a primitive element of H, then $x \in H$. In this case, we consider the generalized degree function μ given by $\mu(x) = 1$, $\mu(y) = N > k$. Let $\{h_1', \ldots, h_m'\}$ be a reduced set of free generators of the subalgebra H with respect to μ. We have $\hat{u} = (x)(\operatorname{Ad} y)^l$. Again, either u is a primitive element of H, or $y \in H$. If $y \in H$, then $H = L(x,y)$. It completes the proof. ■

It is clear that an element u of $[L,L]$ is $\mathfrak{A}$-generic if and only if $u = \sum \alpha_i [f_i, g_i]$, where $\alpha_i \in K$ and the elements $\{f_i, g_i\}$ generate the algebra $L = L(X)$. Therefore, if $u = \sum_{i=1}^s \alpha_i [u_i, v_i]$, where u_i, v_i are monomials of degree greater than one, $\alpha_i \in K$, then u is not a $\mathfrak{A}$-generic element of $L(X)$.

Proposition 13.6.4 ([260]). *Let u be an APE of $L = L(X)$, $u \in [L,L]$. Then u is a $\mathfrak{A}$-generic element of L.*

Proof. Assume that $u \in [H,H]$ for some proper subalgebra H of L. Since u is an APE of L, u is a primitive element of H. But any free generating set of H forms a linear basis of H modulo $[H,H]$. This contradiction proves the statement. ■

Theorem 13.6.5 ([260]). *Let K be a field, $\operatorname{char} K \neq 2$, $X = \{x_1, \ldots, x_n\}$, and $L(X)$ the free Lie algebra over K.*

1) *If $n = 2m$, then*

$$[x_1, x_2] + \cdots + [x_{2m-1}, x_{2m}]$$

is a $\mathfrak{A}$-generic element of $L(X)$.

2) *If $n = 2m$, k_i, l_i, $i = 1, \ldots, m$, are integers, $k_i, l_i \geq 2$, $k_i \neq l_i$, then*

$$u_{k_1,l_1}(x_1,x_2) + \cdots + u_{k_m,l_m}(x_{2m-1}, x_{2m})$$

is a $\mathfrak{A}$-generic element of $L(X)$.

3) *If $n = 2m + 1$ and $l \geq 2$, then*

$$[x_1, x_2] + (x_1)(\operatorname{Ad} x_3)^l + [x_4, x_5] + \cdots + [x_{2m}, x_{2m+1}]$$

is a $\mathfrak{A}$-generic element of $L(X)$.

4) *If $n = 3m$, $l_1, \ldots, l_m \geq 2$, then*

$$[x_1, x_2] + (x_1)(\operatorname{Ad} x_3)^{l_1} + \ldots [x_{3m-2}, x_{3m-1}] + (x_{3m-2})(\operatorname{Ad} x_{3m})^{l_m}$$

is a $\mathfrak{A}$-generic element of $L(X)$.

Proof. Since $k_i, l_i \geq 2$, the elements $u_{k_i,l_i}(x_{2i-1}, x_{2i})$ are μ-homogeneous, where the generalized degree function μ is given by $\mu(x_{2i-1}) = l_i - 1$ and $\mu(x_{2i}) = k_i - 1$. The statements of the theorem follow from Propositions 13.4.6, 13.6.1, 13.6.3, and 13.6.4. ■

Note that if n is even, then $[x_1, x_2] \cdot [x_3, x_4] \cdot \cdots \cdot [x_{n-1}, x_n]$ is a $\mathfrak{A}$-generic element of the free group on $x_1, \ldots, x_n$ [100, 318, 375]; see our Section 3.2.

Let $X = \{x, y\}$, $x > y$, $L = L(x, y)$, $L^{(1)} = [L, L]$, $L^{(2)} = [L^{(1)}, L^{(1)}]$. By Theorem 11.2.8 of Chapter 11, the monomials

$$((x) \operatorname{Ad}^i(y)) \operatorname{Ad}^j(x), \quad i \geq 1, \quad j \geq 0, \tag{13.6}$$

form a set of free generators of the free Lie algebra $L^{(1)}$ (see also [32]).

Lemma 13.6.6. *Let ℓ be a nonzero linear combination of x and y, $L = L(x, y)$. Then:*

1. *If $[g, \ell] \in L^{(2)}$ for a homogeneous element g of L of degree 4, then $g = 0$.*
2. *If $[[[x, y], x], \ell] = [f, \ell_1]$ for some homogeneous element $f \in L$ of degree 3 and a linear element ℓ_1 of L, then either $[\ell, \ell_1] = 0$ or $[\ell_1, x] = 0$.*

Proof.

1. We may assume that $\ell = x$. The element g can be written in the left normed form

$$g = \alpha_1[x, y, y, y] + \alpha_2[x, y, y, x] + \alpha_3[x, y, x, x].$$

Hence

$$[g, l] = \alpha_1[x, y, y, y, x] + \alpha_2[x, y, y, x, x] + \alpha_3[x, y, x, x, x] \in L^{(2)}.$$

Since the elements (13.6) are linearly independent modulo $L^{(2)}$, $\alpha_1 = \alpha_2 = \alpha_3 = 0$, and $g = 0$.

2. Let

$$\begin{aligned} \ell &= \alpha_1 x + \alpha_2 y, & (\alpha_1, \alpha_2) &\neq (0, 0), \\ \ell_1 &= \beta_1 x + \beta_2 y, & (\beta_1, \beta_2) &\neq (0, 0), \\ f &= \gamma_1[[x, y], x] + \gamma_2[[x, y], y], & (\gamma_1, \gamma_2) &\neq (0, 0). \end{aligned}$$

Then the equality $[x, y, x, \ell] = [f, \ell_1]$ is equivalent to the system of equations

$$\alpha_1 = \gamma_1\beta_1, \quad \alpha_2 = \gamma_2\beta_1 + \gamma_1\beta_2, \quad \gamma_2\beta_2 = 0.$$

If $\beta_2 = 0$, then $\ell_1 = \beta_1 x$, and if $\gamma_2 = 0$, then $\ell = \gamma\ell_1$. ■

Theorem 13.6.7 ([260]). *The element*

$$u = [x, y] + [[x, y], x] + [[[x, y], x], [x, y]]$$

is an $\mathfrak{A}$-generic element of the free Lie algebra $L = L(x, y)$, but at the same time it is not an APE of this algebra.

Proof. The element u belongs to the proper subalgebra of L generated by $[x, y]$ and $[[x, y], x]$. It is clear that u is not a primitive element of this subalgebra. Therefore u is not an APE of L.

Suppose that u is not an $\mathfrak{A}$-generic element of L. Then there is a proper subalgebra H of L such that $u \in [H, H]$. By H° we denote the subalgebra of leading terms of elements of H. Since H is generated by some reduced set, if $f \in [H, H]$, then $f^\circ \in [H^\circ, H^\circ]$, and $u^\circ = [[[x, y], x], [x, y]] \in [H^\circ, H^\circ]$. Hence u is a linear combination of homogeneous elements of degree 5 of the form $[f, g]$, where $f, g \in H^\circ$. We may assume that $\mu(f) > \mu(g)$, where μ is usual degree function. If $\mu(g) = 1$, then g is a linear element of L. If H° contains two linearly independent linear elements, then $H = L$. Therefore, we may suppose that $u^\circ = [f, [x, y]] + [g, \ell]$, where ℓ is a linear element. Then $[g, \ell] \in L^{(2)}$. By Lemma 13.6.6, $[g, \ell] = 0$. Hence $f = [[x, y], x]$, and $[[x, y], x], [x, y] \in H^\circ$, and H contain elements of the form $a = [[x, y], x] + \ell_1$, $b = [x, y] + \ell_2$, where ℓ_1 and ℓ_2 are linear elements. Consider the element

$$w = u - [a, b] = [x, y] + [[x, y], x + \ell_1] - [x, y, x, \ell_2] \in [H, H].$$

Suppose that $\ell_2 = 0$. If $x + \ell_1 \neq 0$, then $w^\circ = [[x, y], x + \ell_1] \in [H^\circ, H^\circ]$. It follows that $x + \ell_1 \in H$. Therefore $w - w^\circ = [x, y] \in [H, H]$, and $H = L$. If $x + \ell_1 = 0$, then $[x, y] \in [H, H]$, and again $H = L$.

If $\ell_2 \neq 0$, then

$$w^\circ = -[x, y, x, \ell_2] \in [H^\circ, H^\circ].$$

This is possible only if $[x, y, x, \ell_2] = [g, \ell]$, where ℓ is a nonzero linear element of H, and g is a homogeneous element of H° of degree 3. By Lemma 13.6.6, either $\ell = \alpha\ell_2$ or $\ell = \alpha x$.

If $\ell_2 \in H$, then $[x, y] = b - \ell_2 \in H$. As in the case $\ell_2 = 0$, we get $H = L$. Let $\ell = x \in H$. Then we may assume that $a = [[x, y], x] + \beta y$, $b = [x, y] + \gamma y \in H$, and $0 \neq \gamma \in K$. Therefore

$$a - [b, x] - \gamma b = (\beta - \gamma^2)y \in H.$$

Since $H \neq L$, $\beta = \gamma^2$, and

$$w = u - [a, b] = [x, y] + [[x, y], x + \gamma^2 y] - \gamma[x, y, x, y] \in [H, H].$$

It follows that $w^\circ = -\gamma[x,y,x,y] \in [H^\circ, H^\circ]$. The element $[x,y,x,y]$ has the unique such presentation $[x,y,x,y] = [x,y,y,x]$. Therefore $[[x,y],y] \in H^\circ$, and $c = [[x,y],y] + \delta y \in H$. Consider the element

$$w_1 = w + \gamma[c,x] = (1-\gamma\delta)[x,y] + [[x,y], \alpha + \gamma^2 y] \in [H,H].$$

We have $w_1^\circ = [[x,y], x + \gamma^2 y] \in [H^\circ, H^\circ]$. Therefore $x + \gamma^2 y \in H$. Since $\gamma \neq 0$, $H = L$.

We showed that in all cases $H = L$. Thus u is a $\mathfrak{A}$-generic element of L. ■

Let $\mathfrak{N}_m$ be the variety of nilpotent Lie algebras of degree not less than m. This variety is given by the identity $[x_1, x_2, \ldots, x_m] = 0$, where $[x_1,x_2,x_3] = [[x_1,x_2],x_3], \ldots, [x_1,\ldots,x_m] = [[x_1,\ldots,x_{m-1}],x_m]$.

Theorem 13.6.8 ([260]). *Let $X = \{x_1,\ldots,x_n\}$. The element $u = [x_1,\ldots,x_n]$ is an $\mathfrak{N}_n$-generic element of the free Lie algebra $L(X)$.*

Proof. Let H be a subalgebra of $L(X)$ and $\{h_1,\ldots,h_m\}$ a reduced set of free generators of H. Consider the lower central series of H:

$$\gamma_2(H) = [H,H], \ldots, \gamma_{i+1}(H) = [\gamma_i(H), H].$$

Suppose that the element u belongs to $\gamma_n(H)$. Then

$$u = \sum_{i=1}^{k} [g_1^{(i)}, \ldots, g_n^{(i)}],$$

where $g_1^{(i)}, \ldots, g_n^{(i)} \in H$, $1 \leq i \leq k$. It follows that the element $u^\circ = u$ is a Lie polynomial of degree n in $h_1^\circ, \ldots, h_m^\circ$. It is possible only if u depends on $h_{i_1}, \ldots, h_{i_n}$, $\mu(h_{i_1}) = \cdots = \mu(h_{i_n}) = 1$. But in this case $H = L$. Thus u is an $\mathfrak{N}_n$-generic element. ■

For free groups, the statement of Theorem 13.6.8 was proved by V. Shpilrain [352]. Note that $[x_1,x_2,x_3]$ is an $\mathfrak{N}_3$-generic element of $L(x_1,x_2,x_3)$, but it is not an APE.

Problem 13.6.9. Give complete characterization of generic elements of free Lie algebras. Find an algorithm to determine generic elements.

L. P. Comerford [82] proved that for a variety of groups with algorithmically decidable word problems there is an algorithm to recognize generic elements.

14

Free Leibniz Algebras

Leibniz algebras are possible non-(anti)commutative analogs of Lie algebras. These algebras have appeared in [55] under the name "D-algebras". In [221, 222, 223] J.-L. Loday and T. Pirashvili studied these analogs from the point of view of homological algebra.

Let K be a field and L a K-algebra with the bracket multiplication $[\,,\,]$. Then L is a Leibniz algebra if

$$[x,[y,z]] = [[x,y],z] - [[x,z],y]$$

for all $x, y, z \in L$.

It is obvious that any Lie algebra is a Leibniz algebra, and a Leibniz algebra is a Lie algebra if the condition ($[x,x] = 0$ for all $x \in L$) is fulfilled.

In this chapter, we consider the variety of Leibniz algebras. This variety is not a Schreier variety of algebras. Nevertheless, many combinatorial properties of this variety are similar to the properties of Schreier varieties of algebras.

In Section 14.2, we prove that the variety of all Leibniz algebras has the property of differential separability for subalgebras, Theorem 14.2.1.

We note that Theorem 14.2.1 gives us a negative solution of Problem 2 from [388]: the variety of all Leibniz algebras is not a Schreier variety but has the property of differential separability for subalgebras. In the proof of Theorem 14.2.1, we use some basic facts about standard bases of ideals of free algebras that are not included in this monograph. For these results, we refer to the monographs [33, 57, 275].

Theorem 14.2.2 shows that the Jacobian conjecture has a positive solution for free Leibniz algebras.

In Section 14.3, we study finitely generated subalgebras of the free Leibniz algebra. An algebra R is called residually finite if for any element $a \in R$ and for any finitely generated subalgebra B such that $a \notin B$ there exist a finite dimensional algebra H and a homomorphism $\varphi\colon R \to H$ such that $\varphi(a) \notin \varphi(B)$. Theorem 14.3.8 shows that free Leibniz algebras are residually finite. It follows that the occurrence problem for free Leibniz algebras is decidable.

In order to clarify differences between the variety of Leibniz algebras and Schreier varieties of algebras, we consider automorphisms of free Leibniz algebras in Section 14.4.

Automorphisms of finitely generated free algebras of Schreier varieties of algebras are tame; that is, they are compositions of elementary automorphisms (see Section 11.1 of Chapter 11). To the best of our knowledge, at the moment there are no examples of a non-Schreier variety of algebras all free algebras of which have only tame automorphisms. Possibly, this property characterizes a Schreier variety of algebras.

Automorphisms of two-generated polynomial and free associative algebras are tame (as was proved by H. W. E. Jung [164], W. van der Kulk [194], A. J. Czerniakiewicz [86], and L. G. Makar-Limanov [233]). Examples of wild automorphisms were constructed for the variety of matrix algebras of order 2 (G. Bergman [45] and also the recent article [208] by W. Lee), for the varieties of metabelian, polynilpotent Lie algebras (V. Drensky and C. K. Gupta [101, 105], Yu. A. Bahturin and S. Nabiyev [35], and Yu. A. Bahturin and V. Shpilrain [36]), and for some nilpotent variety of algebras. For more details, we refer to the review article [102] and the monograph [103] by V. Drensky.

We study automorphisms of the free two-generated Leibniz algebra. In Section 14.4.1, Theorem 14.4.5 gives a characterization of tame automorphisms. Section 14.4.2 collects corollaries of the main result. Theorem 14.4.7 shows that there is an algorithm to recognize tame automorphisms. Theorem 14.4.8 gives an example of a wild automorphism.

14.1 Basic Notions

Let X be a set, $F(X)$ the free nonassociative algebra on X over K, and I the two-sided ideal of $F(X)$ generated by the elements

$$[a,[b,c]] - [[a,b],c] - [[a,c],b]$$

for all $a, b, c \in F(X)$. Then the algebra $L(X) = F(X)/I$ is the free Leibniz algebra.

The free Leibniz algebra also has another presentation. Let V be the vector space with the basis X. Then the tensor module

$$T(V) = V \oplus V^{\otimes 2} \oplus \cdots \oplus V^{\otimes n} \oplus \ldots$$

equipped with the bracket multiplication defined inductively by

$$[x, v] = x \otimes v \qquad \text{for } x \in T(V),\ v \in V,$$
$$[x, y \otimes v] = [x, y] \otimes v - [x \otimes v, y] \qquad \text{for } x, y \in T(V),\ v \in V,$$

is the free Leibniz algebra on X.

Let L^l and L^r be two copies of the Leibniz algebra L. We denote by L_x and R_x the elements of L^l and L^r corresponding to the universal operators of left and right multiplication on x. Let I be the two-sided ideal of the associative tensor K-algebra $T(L^l \oplus L^r)$ with the identity element corresponding to the relations

$$R_{[x,y]} = R_x R_y - R_y R_x, \tag{14.1}$$
$$L_{[x,y]} = L_x R_y - R_y L_x, \tag{14.2}$$
$$(R_x + L_x) L_y = 0 \quad \text{for any } x, y \in L. \tag{14.3}$$

Then the factor algebra $UL(L) = T(L^l \oplus L^r)/I$ is the universal multiplicative enveloping algebra of the algebra L in the variety of Leibniz algebras.

Let L^0 be the ideal of the Leibniz algebra L generated by the elements $[x, x]$, where $x \in L$. Then the factor algebra $\bar{L} = L/L^0$ is a Lie algebra. We denote by $\bar{x}$ the image of an element $x \in L$ under the canonical homomorphism $L \to \bar{L}$. Using this homomorphism, we have the homomorphism

$$\bar{}\colon UL(L) \to U(\bar{L}),$$

where $U(\bar{L})$ is the universal enveloping algebra of the Lie algebra $\bar{L}$. In all of what follows we identify the Lie algebra $\bar{L}$ with the corresponding subalgebra of $U(\bar{L})$. Then we get $\bar{R}_x = \bar{x}$, $\bar{L}_x = -\bar{x}$.

Consider the homomorphism

$$\delta\colon U(\bar{L}) \to UL(L)$$

given by $\delta(\bar{x}) = R_x$, $x \in L$.

Since $\overline{\delta(\bar{x})} = \bar{R}_x = \bar{x}$, we identify the algebra $U(\bar{L})$ with the corresponding subalgebra of $UL(L)$.

The algebra $UL(L)$ is a free right $U(\bar{L})$-module with the basis consisting of 1 and the elements L_x, where x runs through the basis of L.

From (14.2) and (14.3), we get

$$L_{[x,y]} = L_x R_y + L_y L_x, \quad \text{where } x, y \in L. \tag{14.4}$$

Consider the mapping

$$d\colon L \to UL(L) \tag{14.5}$$

given by

$$d(x) = L_x \quad \text{with } x \in L.$$

Bearing in mind (14.4), we obtain

$$d([x,y]) = L_{[x,y]} = L_x R_y + L_y L_x = d(x)R_y + d(y)L_x \quad \text{for all} \quad x, y \in L.$$

Therefore, the mapping d is a derivation of the algebra L with coefficients in the $UL(L)$-module $UL(L)$. We set

$$I_L = \{L_x \mid x \in L\} \cdot UL(L);$$

i.e., I_L is the right ideal of the algebra $UL(L)$ generated by the elements L_x, $x \in L$. The mapping $d\colon L \to I_L$ is the universal derivation of the algebra L in the variety of Leibniz algebras. If H is a subalgebra of a Leibniz algebra L, then we set

$$J_H = \{L_x \mid x \in H\} \cdot UL(L).$$

For more details concerning enveloping algebras of Leibniz algebras, we refer to [223].

14.2 Differential Separability of Subalgebras

Theorem 14.2.1 ([258]). *Let x be an element of a Leibniz algebra L and H a subalgebra of L. Then $x \in H$ if and only if $d(x) \in J_H$.*

Proof. We define subsets A, B, C, E of the Leibniz algebra L as follows:

1) A is a basis of the subspace $L^0 \cap H$.

2) $A \cup B$ is a basis of H.

3) $A \cup C$ is a basis of L^0.

4) $A \cup B \cup C \cup E$ is a basis of L.

Consider a linear ordering on the subset $A \cup B \cup C \cup E$ such that from $a \in A$, $b \in B$, $c \in C$, and $e \in E$ it follows that $a < b < c < e$. Let $\bar{B} = \{\bar{b} \mid b \in B\}$, $\bar{E} = \{\bar{e} \mid e \in E\}$. Then the subset $\bar{B} \cup \bar{E}$ is a basis of the algebra $\bar{L}$. By the Poincaré–Birkhoff–Witt theorem, the words

$$w = \bar{b}_{i_1}\bar{b}_{i_2}\ldots\bar{b}_{i_n}\bar{e}_{j_1}\bar{e}_{j_2}\ldots\bar{e}_{j_s}, \tag{14.6}$$

where $b_{i_1} \leq b_{i_2} \leq \cdots \leq b_{i_n}$, $e_{j_1} \leq e_{j_2} \leq \cdots \leq e_{j_s}$, form a basis of the algebra $U(\bar{L})$.

The words

$$L_x w, \tag{14.7}$$

where $x \in A \cup B \cup C \cup E$ and w is as in (14.6), form a basis of the subspace I_L.

Hence the subspace I_L is a free $U(\bar{L})$-module with the basis

$$\{L_x \mid x \in A \cup B \cup C \cup E\}.$$

We see that the words from (14.6) and (14.7) form a basis of the algebra $UL(L)$, and the right ideal J_H of the algebra $UL(L)$ is generated by the elements

$$L_x, \quad x \in A \cup B. \tag{14.8}$$

Therefore the right $U(\bar{L})$-module J_H is generated by the elements from (14.8) and the elements $L_x L_y$, where $x \in A \cup B$ and $y \in A \cup B \cup C \cup E$. From (14.4) we get

$$L_x L_y = -L_y R_x + L_{[y,x]} = -S(x,y),$$

where

$$S(x,y) = L_y \bar{x} - L_{[y,x]}.$$

If $x \in A$, then $R_x = 0$, and $L_x L_y = 0$. Since the subset $A \cup B$ is a basis of the subalgebra H, for $y \in A \cup B$ the element $L_x L_y$ belongs to the $U(\bar{L})$-submodule generated by the elements from (14.8). Thus the elements (14.8) and

$$S(x,y), \quad \text{where} \quad x \in B, \ y \in C \cup E, \tag{14.9}$$

generate the $U(\bar{L})$-module J_H.

The algebra $U(\bar{L})$ is generated by the subset $\bar{B} \cup \bar{E}$ and has the defining relations

$$\bar{x}\bar{z} - \bar{z}\bar{x} - \overline{[x,z]} = 0, \quad \text{where} \quad x, y \in B \cup E, \ x > z. \tag{14.10}$$

Consider the linear ordering on the words from (14.6) and (14.7) at first by the length and then lexicographically.

Elements from (14.9) and (14.10) have the unique composition (in the sense of the composition technique in combinatorial algebra, see monographs [33], [57], and [275]) of the type

$$t = S(x,y)\bar{z} - L_y(\bar{x}\bar{z} - \bar{z}\bar{x} - \overline{[x,z]}),$$

where $x \in B$, $y \in C \cup E$. Since in (14.10) we set $x > z$, $z \in B$,

$$t = S(x,y)\bar{x} + S(x,[y,z]) + S([x,z],y) - S(z,[y,x]),$$

the system of elements from (14.8), (14.9), and (14.10) is a stable system of relations (that is, all possible compositions are resolvable). Then by Shirshov's Composition Lemma (see [33, 57, 349]), if $f \in J_H$, then one of the words

$$L_x, \quad \text{where} \quad x \in A \cup B; \quad L_y \bar{x}, \quad \text{where} \quad x \in B, \ y \in C \cup E,$$

is a beginning subword of the leading word of f. Therefore, if $L_x \in J_H$, then the element L_x is a linear combination of elements (14.8). Thus $x \in H$. ■

Theorem 14.2.2 ([258]). *Let L be the free Leibniz algebra with the set $\{x_1, \ldots, x_n\}$ of free generators and ψ an endomorphism of L. Then*

ψ is an automorphism of L if and only if the Jacobian matrix $J(\psi) = J(\psi(x_1), \ldots, \psi(x_n))$ is invertible over $UL(L)$.

Proof. Let L be the free Leibniz algebra with the free generators $x_1, \ldots, x_n$, and I_L the free $UL(L)$-module with the base $y_1, y_2, \ldots, y_n$. The universal derivation

$$d\colon L \mapsto I_L$$

of the algebra L is given by the rule $d(x_i) = y_i$, $1 \leq i \leq n$. The partial derivatives $\frac{\partial f}{\partial x_i}$ of an element f of the algebra L are given by the following formula:

$$d(f) = \sum_{i=1}^{n} y_i \frac{\partial f}{\partial x_i}, \quad \frac{\partial f}{\partial x_i} \in UL(L).$$

By $\partial(f)$ we denote the column $(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})^{\mathrm{T}}$. Let $f_1, f_2, \ldots, f_n$ be elements of L. By $J(f_1,\ldots,f_n)$ we denote the Jacobian matrix $(\partial(f_1),\ldots,\partial(f_n))$ of these elements. If H is a subalgebra of the algebra L, then we set $J_H = d(H)$. By Theorem 14.2.1, for any $x \in L$ we have that $x \in H$ if and only if $d(x) \in J_H$. Thus the Jacobian conjecture is true for the free Leibniz algebra. ■

Problem 14.2.3. Are the analogs of Theorems 12.5.5 and 12.5.8 valid for free Leibniz algebras?

14.3 Residual Finiteness of Free Leibniz Algebras

Now let L be the free Leibniz algebra with the set $\{x_1, \ldots, x_n\}$ of free generators. By (14.1), (14.2), and (14.3), the algebra $UL(L)$ is generated by the elements

$$L_{x_1}, L_{x_2}, \ldots, L_{x_n}, R_{x_1}, R_{x_2}, \ldots, R_{x_n}. \tag{14.11}$$

These elements satisfy the following relations:

$$(R_{x_i} + L_{x_i})L_{x_j} = 0, \quad 1 \leq i, j \leq n. \tag{14.12}$$

Lemma 14.3.1 ([258]). *The algebra $UL(L)$ is defined by the generators* (14.11) *and defining relations* (14.12). *The words*

$$L_{x_{i_1}} L_{x_{i_2}} \ldots L_{x_{i_k}} R_{x_{j_1}} R_{x_{j_2}} \ldots R_{x_{j_s}}, \quad k, s \geq 0, \tag{14.13}$$

form a basis of the algebra $UL(L)$.

Proof. We set

$$L_{x_1} < L_{x_2} < \cdots < L_{x_n} < R_{x_1} < R_{x_2} < \cdots < R_{x_n}.$$

Then the defining relations (14.12) have no compositions. Hence the algebra given by the generators (14.11) and the defining relations (14.12) has the

basis (14.13). Therefore it is sufficient to prove that the elements (14.13) form a basis of the algebra $UL(L)$.

The elements

$$w = [\dots[[x_{i_1}, x_{i_2}], x_{i_3}], \dots, x_{i_k}], \quad k \geq 1, \tag{14.14}$$

form a basis of the algebra L.

Using the homomorphism δ (see Section 14.1), we identify the algebra $U(\bar{L})$ with the subalgebra of the algebra $UL(L)$ generated by the elements R_{x_i}, $1 \leq i \leq n$. Then the words

$$v = R_{x_{j_1}} R_{x_{j_2}} \dots R_{x_{j_s}}, \quad s \geq 0, \tag{14.15}$$

form a basis of the algebra $U(\bar{L})$.

The elements

$$v,\ L_w v,$$

where v is a word from (14.15) and w is a word from (14.14), form a basis of the algebra $UL(L)$. It follows from (14.2) that

$$L_w = [\dots[[L_{x_{i_1}}, R_{x_{i_2}}], R_{x_{i_3}}], \dots, R_{x_{i_k}}].$$

Then the elements

$$v,\ v_1 L_{x_i} v_2,$$

where v, v_1, v_2 are words from (14.15), $1 \leq i \leq n$, also form a basis of the algebra $UL(L)$. By (14.12), it is possible to change all R-operators in the word v_1 by L-operators. Thus the words (14.13) form a basis of the algebra $UL(L)$. ■

We set $t_i = R_{x_i} + L_{x_i}$, $s_i = L_{x_i}$, $1 \leq i \leq n$. Then the algebra $UL(L)$ is generated by the elements t_i, s_i, and defining relations $t_i s_j = 0$, $1 \leq i, j \leq n$. The words

$$s_{i_1} s_{i_2} \dots s_{i_k} t_{j_1} \dots t_{j_l} \tag{14.16}$$

form a basis of the algebra $UL(L)$. By S and T we denote the free associative subalgebras of the algebra $UL(L)$ generated by the elements $s_1, s_2, \dots, s_n$ and $t_1, t_2, \dots, t_n$, respectively.

Consider the following linear ordering on the words from (14.16), at first by the length and then lexicographically (setting $s_1 < \dots < s_n < t_1 < \dots < t_n$). By $\bar{f}$ we denote the leading term of an element $f \in UL(L)$.

Let u, v be some words from (14.16). We set $u \ll v$ if u is a beginning subword of the word v; i.e., there is a word w from (14.16) such that $v = uw$. In addition, we set $u \prec v$ if there is a word w from (14.16) such that $w \in T$ and $v = u \cdot w$.

Let I be the right ideal of the algebra $UL(L)$ generated by the elements $f_1, \dots, f_k$. Let $g_1, \dots, g_r$ be all elements of the form $f_i s_j$, $1 \leq i \leq k$,

$1 \leq j \leq n$. Then $g_i \in S$ and

$$I = \sum_{i=1}^{k} f_i T + \sum_{j=1}^{r} g_j ST. \tag{14.17}$$

Consider the following system of elements:

$$f_1, \ldots, f_r, g_1, g_2, \ldots, g_r. \tag{14.18}$$

Definition 14.3.2. A system (14.18) of elements of the algebra $UL(L)$ (where $g_i \in S$, $1 \leq i \leq r$) is (f,g)-uncancellable if the following conditions are fulfilled:

a) If $i \neq j$, then $\bar{g}_i \ll \bar{g}_j$ is not the case.

b) For all i, j it is not true that $\bar{g}_i \ll \bar{f}_j$.

c) If $i \neq j$, then $\bar{f}_i \prec \bar{f}_j$ is not the case.

If $\bar{g}_i \ll \bar{g}_j$, then $\bar{g}_j = \bar{g}_i w$, where $w \in S$. Changing g_j by the element $g_j - g_i w$ we get $\overline{g_j - g_i w} < \bar{g}_j$. If $\bar{g}_i \ll \bar{f}_j$ and $\bar{f}_j = \bar{g}_i w$, then we change f_j by $f_j - g_i w$. If now $\bar{f}_i \prec \bar{f}_j$ and $\bar{f}_j = \bar{f}_i w$, $w \in T$, then we change f_j by $f_j - f_i w$. Using such reductions and omitting zero elements, we reduce the system (14.18) to an (f,g)-uncancellable system. The reductions above preserve the equality (14.17).

In all of what follows, we suppose that the system (14.18) is (f,g)-uncancellable.

Lemma 14.3.3 ([258]). *If $h \in I$, then there exists either an element f_i such that $\bar{f}_i \prec \bar{h}$ or an element g_j such that $\bar{g}_j \ll \bar{h}$.*

Corollary 14.3.4 ([258]). *The occurrence problem in finitely generated right ideals of the algebra $UL(L)$ is decidable.*

Using Theorem 14.3.1, we have:

Corollary 14.3.5. *The occurrence problem (in finitely generated subalgebras) is decidable for free Leibniz algebras.*

Definition 14.3.6. We say that an element h of $UL(L)$ is irreducible with respect to the system (14.18) if there are no i, j such that $\bar{f}_i \prec \bar{h}$ or $\bar{g}_j \ll \bar{h}$.

Lemma 14.3.7 ([258]). *If $h \notin I$, then there exists a right ideal J of the algebra $UL(L)$ such that J has finite codimension in $UL(L)$, $I \subseteq J$, and $h \notin J$.*

Proof. We may suppose that the system (14.18) is (f,g)-uncancellable. Moreover, by Lemma 14.3.3, one can assume that the element h is irreducible with respect to the system (14.18). Let m be the maximal length of the elements

$$\bar{h}, \bar{f}_1, \ldots, \bar{f}_k, \bar{g}_1, \ldots, \bar{g}_r.$$

Consider the set of all basic words of the length $m+1$

$$f_{k+1}, f_{k+2}, \dots, f_{k_1}, g_{r+1}, g_{r+2}, \dots, g_{r_1}$$

such that they are irreducible with respect to the system (14.18), $g_i \in S$, $f_j \notin S$.

Then the system

$$f_1, f_2, \dots, f_k, f_{k+1}, \dots, f_{k_1}, g_1, g_2, \dots, g_r, g_{r+1}, \dots, g_{r_1} \tag{14.19}$$

is (f,g)-uncancellable, and the element h is irreducible with respect to the system (14.19).

By J we denote the right ideal of the algebra $UL(L)$ generated by the elements (14.19). Since $f_i ST = f_i T$ with $k+1 \le i \le k_1$,

$$J = \sum_{i=1}^{k_1} f_i T + \sum_{j=1}^{r_1} g_j ST.$$

For any word of length more than m, there exists either f_i, $1 \le i \le k_1$, such that $\bar{f}_i < w$, or g_j, $1 \le j \le r_1$, such that $\bar{g}_j \ll w$. Then the algebra $UL(L)$ is linearly generated by the elements of the length less than $m+1$ (modulo J). Hence the ideal J has finite codimension in $UL(L)$. By Lemma 14.3.3, $h \notin J$. ■

Theorem 14.3.8 ([258]). *The free Leibniz algebras are residually finite.*

Proof. Let L be a finitely generated free Leibniz algebra. Let H be a subalgebra of L generated by elements $h_1, \dots, h_k$. Suppose that $h \notin H$. Then, by Theorem 14.2.1, $d(h) = L_h \notin J_H$. Since d is a derivation, the right ideal J_H is generated by the elements $d(h_1), d(h_2), \dots, d(h_k)$. By Lemma 14.3.7 there exists a right ideal J of the algebra $UL(L)$ such that J has finite codimension in $UL(L)$, $d(h) \notin J$, and $J_H \subseteq J$. Then $M = UL(L)/J$ is a finitely generated $UL(L)$-module. Let $\mathrm{Ann}(M)$ be the annihilator of the module M. Then

$$\mathrm{Ann}(M) \subseteq UL(L) \cdot \mathrm{Ann}(M) \subseteq J_H \cdot UL(L)/\mathrm{Ann}(M)$$

is a finite-dimensional algebra. Therefore the subspace

$$N = \{x \in L \mid R_x, L_x \in \mathrm{Ann}(M)\}$$

has finite codimension in L. Moreover, by (14.1) and (14.2) the subspace N is an ideal of the algebra L. Let $G = L/N$. Now, to complete the proof it is sufficient to show that $h \notin H+N$. On the contrary, assume that $h \in H+N$. Then

$$d(h) \in d(H) + d(N) \subseteq J_H + \mathrm{Ann}(M) \subseteq J,$$

and we come to a contradiction. Let $\varphi\colon L \to G$ be the homomorphism given by $\varphi(x) = x + N$ for $x \in N$. We have that G is a finite-dimensional algebra, and $\varphi(h) \notin \varphi(H)$. ■

14.4 Automorphisms of Free Leibniz Algebras

In this section, we consider automorphisms of two-generated free Leibniz algebras. By $A = LB\langle x_1, x_2\rangle$ we denote the free Leibniz algebra with free generators x_1 and x_2. The monomials

$$[\dots[[x_{i_1}, x_{i_2}], x_{i_3}], \dots, x_{i_k}], \quad i_j = 1, 2,\ 1 \le j \le k,$$

form a linear basis of A. By $UL(A)$ we denote the universal multiplicative enveloping algebra of A.

The algebra A has a structure of a $UL(A)$-module given by $a \cdot r_b = [a, b]$, $a \cdot l_b = [b, a]$ for $a, b \in A$. By $\mathrm{Ann}(A)$ we denote the ideal of A generated by elements $\{[a, a] \mid a \in A\}$. Then $r_a = 0$ if and only if $a \in \mathrm{Ann}(A)$. The algebra $L = A/\mathrm{Ann}(A)$ is the free Lie algebra in two generators. For simplicity, we denote these free generators by x_1 and x_2.

For an element f of A, by $\ell(f)$ we denote the degree of f. Let $\bar{f}$ be the leading homogeneous component of f and $\tilde{f}$ the linear component of f. For an automorphism φ of A given by $\varphi(x_1) = f_1$, $\varphi(x_2) = f_2$, we will use the notation $\varphi = (f_1, f_2)$. The degree $\ell(\varphi)$ of an automorphism $\varphi = (f_1, f_2)$ is the number $\ell(\varphi) = \ell(f_1) + \ell(f_2)$. By $\langle a_1, \dots, a_k\rangle$ we denote the subalgebra of A generated by the elements $a_1, \dots, a_k \in A$.

Lemma 14.4.1 ([3]). *For an automorphism $\varphi = (f_1, f_2)$ of A, we have $f_i - \tilde{f}_i \in \mathrm{Ann}(A)$, $i = 1, 2$.*

Proof. Automorphisms of the free Lie algebra L are tame. Since L has rank 2, these automorphisms are linear. Hence the automorphism φ of A induces a linear automorphism of L. Thus $f_i - \tilde{f}_i \in \mathrm{Ann}(A)$, $i = 1, 2$. ■

Lemma 14.4.2 ([3]). *Let (f_1, f_2) be an automorphism of A, $T(x) \in LB\langle x\rangle$ with $\ell(T(x)) = k$. Then $\ell(T(f_1)) = \ell(f_1) + k - 1$.*

Proof. Let $T(x) = \sum_{i=0}^{k-1} \alpha_i x r_x^i$, where $\alpha_i \in F$, $\alpha_{k-1} \neq 0$. By Lemma 14.4.1, $f_1 - \tilde{f}_1 \in \mathrm{Ann}(A)$, and therefore $r_{f_1} = r_{\tilde{f}_1}$. Hence

$$T(f_1) = \sum_{i=0}^{k-1} \alpha_i f_1 r_{f_1}^i = \sum_{i=0}^{k-1} \alpha_i f_1 r_{\tilde{f}_1}^i;$$

that is, $\overline{T(f_1)} = \alpha_{k-1} \bar{f}_1 r_{\tilde{f}_1}^{k-1}$. Thus $\ell(T(f_1)) = \ell(f_1) + k - 1$. ■

14.4.1 Simple automorphisms

We recall that an elementary transformation of a set $\{f_1, f_2, \dots\}$ is a change of one element f_i by an element $\alpha f_i + g$, where $0 \neq \alpha \in F$, $g \in \langle\{f_j \mid j \neq i\}\rangle$. If $\{g_1, g_2\}$ is the result of applying one elementary transformation to $\{f_1, f_2\}$, then we write $(f_1, f_2) \to (g_1, g_2)$. If (f_1, f_2) is a tame

automorphism of A, then there is a series of elementary automorphisms

$$(x_1, x_2) = (f_1^{(0)}, f_2^{(0)}) \to (f_1^{(1)}, f_2^{(1)}) \to \cdots \to (f_1^{(k)}, f_2^{(k)}) = (f_1, f_2).$$

Definition 14.4.3. Let (f_1, f_2) be an automorphism of A. We say that the element f_1 is (elementary) reducible if there are $\alpha \in F$, $\alpha \neq 0$, and $g \in \langle f_2 \rangle$ such that $\ell(\alpha f_1 + g) < \ell(f_1)$. We say also that the element f_1 is reducible by the automorphism $(\alpha f_1 + g, f_2)$.

Definition 14.4.4. We define simple automorphisms of A by induction on the degree as follows.

1. Linear automorphisms of A are simple.
2. Suppose that we have defined simple automorphisms of degree less than k ($k \geq 2$). An automorphism (f_1, f_2) of A of degree k is simple if f_1 or f_2 is reducible by a simple automorphism.

An element f_i of the automorphism (f_1, f_2) is said to be simple reducible if it is reducible by a simple automorphism.

Theorem 14.4.5 ([3]). *Tame automorphisms of the free two-generated Leibniz algebra $A = LB\langle x_1, x_2 \rangle$ are simple.*

Proof. Assume the contrary. Then there is a sequence of elementary automorphisms

$$(x_1, x_2) = (f_1^{(0)}, f_2^{(0)}) \to (f_1^{(1)}, f_2^{(1)}) \to \cdots \to (f_1^{(k)}, f_2^{(k)}) \to (f_1^{(k+1)}, f_2^{(k+1)}) \tag{14.20}$$

such that the automorphism $\theta = (f_1^{(k+1)}, f_2^{(k+1)})$ is not simple, and at the same time all automorphisms $\theta_i = (f_1^{(i)}, f_2^{(i)})$, $1 \leq i \leq k$, are simple. Let $\mathcal{M}$ be the set of all such sequences. We say that $\ell(\theta_k) = \ell(f_1^{(k)}) + \ell(f_2^{(k)})$ is the control number of the sequence (14.20). Suppose that a sequence (14.20) has the minimal possible control number. We show that θ is a simple automorphism. Let

$$(g_1, g_2) = (f_1^{(k-1)}, f_2^{(k-1)}), \quad (f_1, f_2) = (f_1^{(k)}, f_2^{(k)}).$$

We may suppose that

$$f_1 = f_1^{(k+1)}, \quad f_2^{(k+1)} = f = f_2 + g, \quad g = T(f_1) \in \langle f_1 \rangle. \tag{14.21}$$

Since θ_k is simple, f_1 or f_2 is simple reducible (by θ_k). Assume that f_2 is simple reducible. Then we may suppose that f_2 is reducible by θ_{k-1}; that is, $g_1 = f_1$, $g_2 = f_2 - S(f_1)$, $\ell(g_2) < \ell(f_2)$. Therefore we may change the two last automorphisms of the sequence (14.20) by one automorphism:

$$\theta_{k-1} = (g_1, g_2) \to (g_1, g_2 + S(g_1) + T(g_1)) = (f_1, f) = \theta.$$

Since the control number of the new sequence is less than $\ell(\theta_k)$, the automorphism $\theta = (f_1, f)$ is simple. Hence f_2 is not simple reducible by θ_k.

Therefore we may assume that f_1 is reducible by θ_{k-1},

$$g_1 = f_1 - S(f_2), \quad g_2 = f_2, \quad \ell(g_1) < \ell(f_1). \tag{14.22}$$

If $\ell(g) > \ell(f_2)$ in (14.21), then the element f of the automorphism θ is reducible by the simple automorphism θ_k. Therefore we suppose that $\ell(d) \leq \ell(f_2)$. By Lemma 14.4.2, $\ell(g) = \ell(T(f_1)) = \ell(f_1) + \ell(T(x)) - 1$. Therefore, we have to consider the following cases:

(a) $\ell(f_1) = \ell(f_2)$, $\ell(T(x)) = 1$;

(b) $\ell(f_1) < \ell(f_2)$, $\ell(T(x)) > 1$.

It follows from (14.22) that $\bar{f}_1 = \overline{S(f_2)}$; that is, $\ell(f_2) \leq \ell(f_1)$. Thus we have to consider only the case where $\ell(f_1) = \ell(f_2)$, $T(x) = \alpha x$, $S(x) = \beta x$, $\alpha, \beta \in F$, $g_1 = f_1 - \beta f_2$, $\bar{f}_1 = \beta \bar{f}_2$, $f = f_2 + \alpha f_1$. Let $\gamma = 1 + \alpha\beta$. Then $f = \gamma f_2 + \alpha g_1$, $\gamma f_1 = \beta f + g_1$. If $\gamma \neq 0$, then we change the last two transformations of (14.20) by

$$\theta_{k-1} = (g_1, g_2) = (g_1, f_2) \to (g_1, f) \to (f_1, f) = \theta.$$

Since $\ell(g_1) + \ell(g_2) < \ell(\theta_k)$, (g_1, f) is a simple automorphism. It follows from $\ell(g_1) + \ell(f) < \ell(f_1) + \ell(f_2) = \ell(\theta_k)$ that the automorphism θ is simple.

If $\gamma = 0$, then $f = \alpha g_1$, $f_1 = \frac{1}{\alpha} f + \beta g_2$. Since (g, g_2) is a simple automorphism, $(\alpha g_1, g_2) = (f, g_2)$ is also a simple automorphism. Moreover, the automorphism (g_2, f) is simple.

Consider the elementary transformation $(g_2, f) \to (f_1, f) = \theta$. Taking into account that

$$\ell(g_2) + \ell(f) = \ell(g_2) + \ell(g_1) < \ell(\theta_{k-1}),$$

by the choice of (14.20), θ is a simple automorphism. ■

14.4.2 Recognizing tame automorphisms

Results of this section are corollaries of Theorem 14.4.5.

Proposition 14.4.6. *Let (f_1, f_2) be a tame automorphism of A, $\ell(f_1) + \ell(f_2) > 2$. Then there is i, $i = 1, 2$, and an element g of $\langle \{f_j \mid j \neq i\} \rangle$ such that $\bar{f}_i = \bar{g}$.*

Proof. By Theorem 14.4.5, the automorphism (f_1, f_2) is simple. Suppose that f_1 is a reducible element. Then there is $g \in \langle f_2 \rangle$ such that $\ell(f_1 - g) < \ell(f_1)$. Thus $\bar{f}_1 = \bar{g}$. ■

Theorem 14.4.7 ([3]). *If the field K is constructive, then there is an algorithm to recognize tame and wild automorphisms of A.*

Proof. By Lemma 14.4.1, the statement of Proposition 14.4.6 can be algorithmically verified. ■

Proposition 14.4.6 gives us a possibility to construct a series of wild automorphisms of the algebra A. An example of a wild automorphism of the minimal degree is given by the following theorem:

Theorem 14.4.8 ([3]). *The automorphism* $(x_1 + [[x_2, x_2], x_1], x_2)$ *of* A *is wild.*

Proof. Let $f_1 = x_1 + [[x_2, x_2], x_1]$, $f_2 = x_2$. Since $[[f_2, f_2], f_1] = [[x_2, x_2], x_1]$, (f_1, f_2) is an automorphism of A. At the same time, (f_1, f_2) does not satisfy the statement of Proposition 14.4.6. ■

References

[1] A. T. Abdykhalykov, *Magnus embedding for Leibniz algebras.* Science and Education of South Kazakhstan. Math. **6** (1997), 218–224.

[2] A. T. Abdykhalykov, *The occurrence problem for free solvable Leibniz algebras.* Vestnik Kaz. Univ. Ser. Mat., Mekh., Inf. **23** (2000), no. 4, 19–25.

[3] A. T. Abdykhalykov, A. A. Mikhalev, and U. U. Umirbaev, *Automorphisms of two-generated free Leibniz algebras.* Commun. Algebra **29** (2001), 2953–2960.

[4] S. S. Abhyankar, *Algebraic Geometry for Scientists and Engineers.* American Mathematical Society, Providence, 1990.

[5] S. S. Abhyankar, *Expansion Techniques in Algebraic Geometry.* Tata Institute of Fundamental Research, Bombay, 1977.

[6] S. S. Abhyankar, *Lectures on Expansion Techniques in Algebraic Geometry*, Notes by Balwant Singh. Tata Institute of Fundamental Research Lectures on Mathematics and Physics **57**. Tata Institute of Fundamental Research, Bombay, 1977.

[7] S. S. Abhyankar, *On the semigroup of a meromorphic curve. I.* In: M. Nagata (ed.), *Proceedings of the International Symposium on Algebraic Geometry (Kyoto University, Kyoto, 1977).* Kinokuniya Book Store, Tokyo, 1978, 249–414.

[8] S. S. Abhyankar, P. Eakin, and W. J. Heinzer, *On the uniqueness of the coefficient ring in a polynomial ring.* J. Algebra **23** (1972), 310–342.

[9] S. S. Abhyankar and W. Li, *On the Jacobian conjecture: A new approach via Gröbner bases.* J. Pure Appl. Algebra **61** (1989), 211–222.

[10] S. S. Abhyankar and T. T. Moh, *Embedding of the line in the plane.* J. Reine Angew. Math. **276** (1975), 148–166.

[11] S. S. Abhyankar and A. Sathaye, *Uniqueness of plane embeddings of special curves.* Proc. Amer. Math. Soc. **124** (1996), 1061–1069.

[12] S. S. Abhyankar and B. Singh, *Embeddings of certain curves in the affine plane.* Amer. J. Math. **100** (1978), 99–175.

[13] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases.* Graduate Studies in Mathematics **3**. American Mathematical Society, Providence, 1994.

[14] S. A. Agalakov, *A Lie algebra with one defining relation need not be residually finite.* Mat. Zametki **51** (1992), no. 4, 3–7, 139. English translation: in Math. Notes.

[15] J. Alev, *A note on Nagata's automorphism.* In: A. van den Essen (ed.), *Automorphisms of Affine Spaces.* Kluwer Academic Publishers, Dordrecht, 1995, 215–221.

[16] D. J. Anick, *Limits of tame automorphisms in* $k[x_1, \ldots, x_N]$. J. Algebra **82** (1983), 459–468.

[17] H. Appelgate and H. Onishi, *The Jacobian conjecture in two variables.* J. Pure Appl. Algebra **37** (1985), 215–227.

[18] E. Artal-Bartolo, P. Cassou-Nogues, and I. Luengo Velasco, *On polynomials whose fibers are irreducible with no critical points.* Math. Ann. **299** (1994), 477–490.

[19] V. A. Artamonov, *Nilpotency, projectivity, freeness.* Vestnuk Moscow Univ. Ser. I. Math. Mech. **26** (1971), no. 5, 50–53.

[20] V. A. Artamonov, *Projective metabelian groups and Lie algebras.* Izv. Akad. Nauk SSSR Ser. Mat. **42** (1978), no. 2, 226–236. English translation: USSR-Izv. **42** (1978), 213–223.

[21] V. A. Artamonov, *Nilpotency, projectivity and decomposability.* Sibirsk. Mat. Zh. **32** (1991), no. 6, 3–11. English translation: Siberian Math. J. **32** (1991), no. 6, 901–909.

[22] V. A. Artamonov, *Projective metabelian D-groups and Lie superalgebras.* Trudy Semin. Im. I. G. Petrovskogo **15** (1991), 189–195. English translation: J. Soviet Math. **60** (1992), no. 6, 1790–1795.

[23] V. A. Artamonov, *The Magnus representation in congruence modular varieties.* Sibirsk. Mat. Zh. **38** (1997), no. 5, 978–995. English translation: Siberian Math. J. **38** (1997), 842–859.

[24] V. A. Artamonov, *Transitivity of action on modular vectors.* Fundam. Prikl. Mat. **5** (1999), no. 3, 765–773.

[25] V. A. Artamonov, *Varieties of Algebras.* In: M. Hazenwinkel (ed.), *Handbook of Algebra. Vol. 2.* Elsevier, Amsterdam, 2000, 545–575.

[26] V. A. Artamonov and M. S. Burgin, *Some properties of subalgebras in varieties of linear* Ω*-algebras.* Mat. Sb. **87** (1972), no. 1, 67–82. English translation: Math. USSR Sb. **16** (1972), 69–85.

[27] V. A. Artamonov, A. A. Mikhalev, and A. V. Mikhalev, *Combinatorial properties of free algebras of Schreier varieties.* In: *Polynomial Identities and Combinatorial Methods.* Marcel Dekker, New York, 2003, 47–99.

[28] T. Asanuma, *Non-linearizable algebraic k^*-actions on affine spaces.* Invent. Math. **138** (1999), 281–306.

[29] S. Bachmuth, E. Formanek, and H. Y. Mochizuki, *IA-automorphisms of certain two-generator torsion-free groups.* J. Algebra **40** (1976), 19–30.

[30] Yu. A. Bahturin, *Two remarks on Lie algebra varieties.* Mat. Zametki **4** (1968), 387–398.

[31] Yu. A. Bahturin, *Identities in Lie algebras, I.* Vestnik Moskov. Univ. Ser. I. Mat. Mekh. **28** (1973), no. 1, 12–18. English translation: Moscow Univ. Math. Bull. **28** (1973), no. 1, 9–15.

[32] Yu. A. Bahturin, *Identical Relations in Lie Algebras.* VNU Science Press, Utrecht, 1987.

[33] Yu. A. Bahturin, A. A. Mikhalev, V. M. Petrogradsky, and M. V. Zaicev, *Infinite Dimensional Lie Superalgebras.* Walter de Gruyter, Berlin–New York, 1992.

[34] Yu. A. Bahturin, A. A. Mikhalev, and M. V. Zaicev. *Infinite-dimensional Lie superalgebras.* In: M. Hazelwinkel (ed.), *Handbook of Algebra, Vol. 2.* Elsevier, Amsterdam, 2000, 579–614.

[35] Yu. A. Bahturin and S. Nabiyev, *Automorphisms and derivations of abelian extensions of some Lie algebras.* Abh. Math. Semin. Univ. Hamburg **62** (1992), 43–57.

[36] Yu. A. Bahturin and V. Shpilrain, *On Lie algebras with wild automorphisms.* Results Math. **28** (1995), nos. 3–4, 209–213.

[37] T. Bandman and L. Makar-Limanov, *Affine surfaces with isomorphic cylinders.* Preprint.

[38] T. M. Baranovich and M. S. Burgin, *Linear Ω-algebras.* Uspehi Mat. Nauk **30** (1975), no. 4, 61–106. English translation: Russian Math. Surveys **30** (1975), no. 4, 65–113.

[39] H. Bass, E. Connell, and D. Wright, *The Jacobian conjecture: reduction on degree and formal expansion of the inverse.* Bull. Amer. Math. Soc. **7** (1982), 287–330.

[40] G. Baumslag, *On generalised free products.* Math. Z. **78** (1962), 423–438.

[41] G. Baumslag, A. G. Myasnikov, and V. Remeslennikov, *Algebraic geometry over groups. I. Algebraic sets and ideal theory.* J. Algebra **219** (1999), 16–79.

[42] G. Baumslag, A. G. Myasnikov, and V. Shpilrain, *Open problems in combinatorial group theory.* In: R. Gilman (ed.), *Groups, Languages and Geometry (South Hadley, MA, 1998)*, Contemporary Mathematics **250**. American Mathematical Society, Providence, 1999, 1–27.

[43] G. Baumslag, A. G. Myasnikov, and V. Shpilrain, *Open problems in combinatorial group theory, Second edition.* Contemporary Mathematics **296**. American Mathematical Society, Providence, 2002, 1–38.

[44] K. Bencsath, B. Fine, A. M. Gaglione, A. G. Myasnikov, F. Roehl, G. Rosenberger, and D. Spellman, *Aspects of the theory of free groups.* In: J. C. Birget, S. Margolis, J. Meakin, and M. Sapir (eds.), *Algorithmic Problems in Groups and Semigroups.* Birkhäuser, Boston, 2000, 51–90.

[45] G. M. Bergman, *Wild automorphisms of free P.I. algebras, and some new identities.* Preprint.

[46] G. M. Bergman, *An Invitation to General Algebra and Universal Constructions.* Henry Helson, Berkeley, CA, 1998.

[47] G. M. Bergman, *Supports of derivations, free factorizations, and ranks of fixed subgroups in free groups.* Trans. Amer. Math. Soc. **351** (1999), 1531–1550.

[48] G. M. Bergman and W. Dicks, *On universal derivations.* J. Algebra **36** (1975), 193–211.

[49] G. M. Bergman and W. Dicks, *Universal derivations and universal ring constructions.* Pacific J. Math. **79** (1978), no. 2, 293–337.

[50] J. Berson, *Stably tame coordinates.* J. Pure Appl. Algebra **170** (2002), 131–143.

[51] M. Bestvina and M. Handel, *Train tracks and automorphisms of free groups.* Ann. Math. **135** (1992), no. 2, 1–51.

[52] A. Bialynicki-Birula and M. Rosenlicht, *Injective morphisms of real algebraic varieties.* Proc. Amer. Math. Soc. **13** (1962), 200–203.

[53] R. Bieri and B. Eckmann, *Relative homology and Poincaré duality for group pairs.* J. Pure Appl. Algebra **13** (1978), 277–319.

[54] J. S. Birman, *An inverse function theorem for free groups.* Proc. Amer. Math. Soc. **41** (1973), 634–638.

[55] A. Bloh, *On a generalization of the concept of Lie algebra.* Dokl. Akad. Nauk SSSR **165** (1965), 471–473.

[56] S. Bochner and W. T. Martin, *Several Complex Variables.* Princeton University Press, Princeton, 1948.

[57] L. A. Bokut' and G. P. Kukin, *Algorithmic and Combinatorial Algebra.* Kluwer Academic Publishers, Dordrecht, 1994.

[58] A. Borovik, A. G. Myasnikov, and V. Shpilrain, *Measuring Sets in Infinite groups.* Contemporary Mathematics **298**. American Mathematical Society, Providence, 2002, 21–42.

[59] A. Braun, *The nilpotency of the radical in a finitely generated PI-ring.* J. Algebra **89** (1984), 375–396.

[60] A. M. Brunner, R. G. Burns, and S. Oates-Williams, *On almost primitive elements of free groups with an application to Fuchsian groups.* Can. J. Math. **45** (1993), 225–254.

[61] R. M. Bryant and V. Drensky, *Dense subgroups of the automorphism groups of free algebras.* Can. J. Math. **45** (1993), 1135–1154.

[62] G. Burde and H. Zieschang, *Knots.* De Gruyter Studies in Mathematics **5**. Walter de Gruyter & Co., Berlin–New York, 1985.

[63] J. Burillo and E. Ventura, *Counting primitive elements in free groups*, Geom. Dedicata **93** (2002), 143–162.

[64] L. A. Campbell, *A condition for a polynomial map to be invertible.* Math. Ann. **205** (1973), 243–248.

[65] A. Campbell and J.-T. Yu, *Two-dimensional coordinate polynomials and dominant maps.* Commun. Algebra **28** (2000), 2297–2301.

[66] K. Champagnier, *Algorithms to realize the rank and primitivity of a system of elements in free non-associative algebras.* Fundam. Prikl. Mat. **6** (2000), 1229–1238.

[67] K. Champagnier, *Ranks of subalgebras of free non-associative algebras.* Commun. Algebra, to appear.

[68] C. C. Cheng and A. van den Essen, *Endomorphisms of the plane sending linear coordinates to coordinates.* Proc. Amer. Math. Soc. **128** (2000), 1911–1915.

[69] C. Cheng and S. Wang, *An algorithm that determines whether a polynomial map is bijective.* In: A. van den Essen (ed.), *Automorphisms of Affine Spaces.* Kluwer Academic Publishers, Dordrecht, 1995, 169–176.

[70] I. V. Chirkov and M. A. Shevelin, *Test sets in free metabelian Lie algebras.* Sibirsk. Mat. Zh. **43** (2002), no. 6, 1401–1407. English translation: Siberian Math. J. **43** (2002), no. 6, 1135–1140.

[71] M. Cohen, W. Metzler, and B. Zimmermann, *What does a basis of $F[a, b]$ look like?* Math. Ann. **257** (1981), 435–445.

[72] H. Cohn, *Markoff forms and primitive words.* Math. Ann. **196** (1972), 8–22.

[73] P. M. Cohn, *On homomorphic images of special Jordan algebras.* Can. J. Math. **6** (1954), 253–264.

[74] P. M. Cohn, *On a generalization of the Euclidean algorithm.* Proc. Cambridge Philos. Soc. **57** (1961), 18–30.

[75] P. M. Cohn, *Rings with a weak algorithm.* Trans. Amer. Math. Soc. **109** (1963), 332–356.

[76] P. M. Cohn, *Free ideal rings.* J. Algebra **1** (1964), 47–69.

[77] P. M. Cohn, *Subalgebras of free associative algebras.* Proc. London Math. Soc. **14** (1964), no. 3, 618–632.

[78] P. M. Cohn, *On the structure of the* GL_2 *of a ring.* Inst. Hautes Études Sci. Publ. Math. **30** (1966), 365–413.

[79] P. M. Cohn, *Universal Algebra, 2nd Ed.* Reidel, Dordrecht, 1981.

[80] P. M. Cohn, *Free Rings and Their Relations, 2nd Ed.* Academic Press, London, 1985.

[81] P. M. Cohn, *Skew Fields. Theory of General Division Rings.* Cambridge University Press, Cambridge, 1995.

[82] L. P. Comerford, *Generic elements of free groups.* Arch. Math. (Basel) **65** (1995), 185–195.

[83] E. Connell and J. Zweibel, *Subrings invariant under polynomial maps.* Houston J. Math. **20** (1994), 175–185.

[84] D. Costa, *Retracts of polynomial rings.* J. Algebra **44** (1977), 492–502.

[85] R. Crowell and R. Fox, *Introduction to Knot Theory.* Graduate Texts in Mathematics **57**. Springer-Verlag, New York–Heidelberg, 1977.

[86] A. J. Czerniakiewicz, *Automorphisms of a free associative algebra of rank* 2, *I, II.* Trans. Amer. Math. Soc. **160** (1971), 393–401; **171** (1972), 309–315.

[87] D. Daigle and G. Freudenburg, *Locally nilpotent derivations over a UFD and an application to rank two locally nilpotent derivations of* $k[X_1, \ldots, X_n]$. J. Algebra **204** (1998), 353–371.

[88] W. Danielewski, *On the cancellation problem and automorphism groups of affine algebraic varieties.* Preprint, Warsaw, 1989.

[89] A. N. Danilov, *On Magnus presentation for non-associative algebras.* Vestnik Moskov. Univ. Ser. I. Mat. Mekh. (2003), no. 2, 50–52. English translation: Moscow Univ. Math. Bull.

[90] H. Derksen, F. Kutzschebauch, and J. Winkelmann, *Subvarieties of* $\mathbb{C}^n$ *with non-extendable automorphisms.* J. Reine Angew. Math. **508** (1999), 213–235.

[91] J. Désarménien, G. Duchamp, D. Krob, and G. Melançon, *Quelques remarques sur les super-algèbres de Lie libres.* C. R. Acad. Sci. Paris. Sér. I Math. **318** (1994), 419–424.

[92] W. Dicks, *On one-relator associative algebras.* J. London Math. Soc. **5** (1972), no. 2, 249–252.

[93] W. Dicks, *A commutator test for two elements to generate the free algebra of rank two.* Bull. London Math. Soc. **14** (1982), 48–51.

[94] W. Dicks, *Automorphisms of the polynomial ring in two variables.* Publ. Sec. Mat. Univ. Autonoma Barcelona **27** (1983), 155–162.

[95] W. Dicks and M. J. Dunwoody, *Groups Acting on Graphs.* Cambridge University Press, Cambridge, 1989.

[96] W. Dicks and J. Lewin, *A Jacobian conjecture for free associative algebras.* Commun. Algebra **10** (1982), 1285–1306.

[97] T. tom Dieck and T. Petrie, *Contractible affine surfaces of Kodaira dimension one.* Japan J. Math. **16** (1990), 147–169.

[98] N. Dobrynin, *The free color Lie superstructures: elimination of variables.* In: Y. Fong, A. V. Mikhalev, and E. Zelmanov (eds.), *Lie Algebras, Rings and Related Topics.* Springer, Hong Kong, 2000, 32–48.

[99] N. Dobrynin, G. Duchamp, A. A. Mikhalev, and V. Petrogradsky, *On free p-superalgebras.* Commun. Algebra **28** (2000), 5275–5302.

[100] A. Dold, *Nullhomologous words in free groups which are not nullhomologous in any proper subgroup*, Arch. Math. **50** (1988), 564–569.

[101] V. Drensky, *Automorphisms of relatively free algebras.* Commun. Algebra **18** (1990), 4323–4351.

[102] V. Drensky, *Endomorphisms and automorphisms of relatively free algebras.* Suppl. Rend. Circ. Mat. Palermo **31** (1993), 97–132.

[103] V. Drensky, *Free Algebras and PI-Algebras: Graduate Course in Algebra.* Springer-Verlag, Singapore, 2000.

[104] V. Drensky, A. van den Essen, and D. Stefanov, *New stably tame automorphisms of polynomial algebras.* J. Algebra **226** (2000), 629–638.

[105] V. Drensky and C. K. Gupta, *Automorphisms of free nilpotent Lie algebras.* Can. J. Math. **17** (1990), 259–279.

[106] V. Drensky, J. Gutierrez, and J.-T. Yu, *Gröbner basis and the Nagata automorphism.* J. Pure Appl. Algebra **135** (1999), 135–153.

[107] V. Drensky, V. Shpilrain, and J.-T. Yu, *On the density of the set of generators of a polynomial algebra.* Proc. Amer. Math. Soc. **128** (2000), 3465–3469.

[108] V. Drensky and J.-T. Yu, *Exponential automorphisms of polynomial algebras.* Commun. Algebra **26** (1998), 2977–2985.

[109] V. Drensky and J.-T. Yu, *Orbits in free algebras of rank two.* Commun. Algebra **26** (1998), 1895–1906.

[110] V. Drensky and J.-T. Yu, *Test polynomials for automorphisms of polynomial and free associative algebras.* J. Algebra **207** (1998), 491–510.

[111] V. Drensky and J.-T. Yu, *Automorphisms and coordinates of polynomial algebras.* Contemporary Mathematics **264**. American Mathematical Society, Providence, 2000, 179–206.

[112] V. Drensky and J.-T. Yu, *Tame and wild coordinates of* $K[z][x, y]$. Trans. Amer. Math. Soc. **353** (2001), 519–537.

[113] L. M. Druźkowski, *The Jacobian conjecture in case of rank or corank less than three.* J. Pure Appl. Algebra **85** (1993), 233–244.

[114] G. Duchamp and D. Krob, *The free partially commutative Lie algebra: bases and ranks.* Adv. Math. **95** (1992), no. 1, 92–126.

[115] V. G. Durnev, *The Maltsev–Nielsen equation in a free metabelian group of rank two.* Mat. Zametki **46** (1989), no. 6, 57–60. English translation: Math. Notes **46** (1989), 927–929.

[116] V. G. Durnev, *On the problem of the solvability of equations with one coefficient.* Mat. Zametki **59** (1996), no. 6, 832–845. English translation: Math. Notes **59** (1996), 601–610.

[117] B. Eckmann and H. Müller, *Poincaré duality groups of dimension* 2. Comment. Math. Helv. **55** (1980), 510–520.

[118] E. Engel, *Ein Satz über ganze Gremona Transformation der Ebene.* Math. Ann. **130** (1955), 11–19.

[119] A. van den Essen, *A criterion to decide if a polynomial map is invertible and to compute the inverse.* Commun. Algebra **18** (1990), 3183–3186.

[120] A. van den Essen, *Locally nilpotent derivations and their applications, III.* J. Pure Appl. Algebra **98** (1995), 15–23.

[121] A. van den Essen, *Seven Lectures on Polynomial Automorphisms.* In: A. van den Essen (ed.), *Automorphisms of Affine Spaces. Proceedings of the Conference "Invertible Polynomial Maps", July 1994, Curaçao.* Kluwer Academic Publishers, Dordrecht, 1995, 3–39.

[122] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture.* Progress in Mathematics **190**. Birkhäuser Verlag, Basel, 2000.

[123] A. van den Essen and M. Kwiecinski, *On the reconstruction of polynomial automorphisms from their face polynomials.* J. Pure Appl. Algebra **80** (1992), 327–336.

[124] A. van den Essen and V. Shpilrain, *Some combinatorial questions about polynomial mappings.* J. Pure Appl. Algebra **119** (1997), 47–52.

[125] A. van den Essen and H. Tutaj, *A remark on the two-dimensional Jacobian conjecture.* J. Pure Appl. Algebra **96** (1994), 19–22.

[126] T. Evans, *Word problems.* Bull. Amer. Math. Soc. **84** (1978), 789–802.

[127] G. L. Feldman, *Ends of Lie algebras.* Uspekhi Mat. Nauk **38** (1983), no. 1, 199–200. English translation: Russian Math. Surveys **38** (1983), no. 1, 182–184.

[128] K.-Q. Feng and J.-T. Yu, *New classes of test polynomials of polynomial algebras.* Sci. China Ser. A **42** (1999), 712–719.

[129] M. Fiedler and V. Pták, *On matrices with non-positive off-diagonal elements and positive principal minors.* Czech. Math. J. **12** (1962), 382–400.

[130] K.-H. Fieseler, *On complex affine surfaces with $\mathbb{C}^+$-action.* Comment. Math. Helv. **69** (1994), 5–27.

[131] B. Fine, G. Rosenberger, D. Spellman, and M. Stille. *Test, generic and almost primitive elements in free groups.* Contemp. Math. **14** (1998), 45–59.

[132] B. Fine, G. Rosenberger, D. Spellman, and M. Stille, *Test words, generic elements and almost primitivity*, Pacific J. Math. **190** (1999), 277–297.

[133] E. Formanek, *Observations about the Jacobian conjecture.* Houston J. Math. **20** (1994), 369–380.

[134] R. H. Fox, *Free differential calculus. I. Derivations in free group rings.* Ann. Math. **57** (1953), no. 2, 547–560.

[135] R. H. Fox, *Free differential calculus. III. Subgroups.* Ann. Math. **64** (1956), no. 2, 407–419.

[136] G. Freudenburg, *Triangulability criteria for additive group actions on affine space.* J. Pure Appl. Algebra **105** (1995), 267–275.

[137] G. Freudenburg, L. Moser-Jauslin, *Non-equivalent embeddings of Danielewski surfaces and non-linearizable actions of $\mathcal{O}(2)$ on $\mathbb{C}^4$.* Math. Z., to appear.

[138] T. Fujita, *On Zariski problem*, Proc. Japan Acad. Ser. A Math. Sci. **55** (1979), 106–110.

[139] A. T. Gainov, *Commutative free and anti-commutative free products of algebras.* Dokl. Akad. Nauk SSSR **133** (1960), no. 6, 1275–1278.

[140] A. T. Gainov, *Derivations of reduced free algebras.* Algebra i Logika **1** (1962/1963), no. 6, 20–25.

[141] V. N. Gerasimov, *Distributive lattices of subspaces and the word problem for one-relator algebras.* Algebra i Logika **15** (1976), no. 4, 384–435. English translation: Algebra and Logic **15** (1976), 238–274.

[142] V. N. Gerasimov, *Free associative algebras and inverting homomorphisms of rings.* In: V. N. Gerasimov, N. G. Nesterenko, and A. I. Valitskas (eds.), *Three Papers on Algebras and Their Representations.* American Mathematical Society, Providence, 1993, 1–76.

[143] G. Grätzer, *Universal Algebra, 2nd Ed.* Springer-Verlag, New York, 1979.

[144] C. K. Gupta and E. I. Timoshenko, *Primitivity in the free groups of the variety $\mathcal{A}_m\mathcal{A}_n$*. Commun. Algebra **24** (1996), 2859–2876.

[145] C. K. Gupta and E. I. Timoshenko, *Automorphic and endomorphic reducibility and primitive endomorphisms*. Commun. Algebra **25** (1997), 3057–3070.

[146] N. Gupta, *Free Group Rings*. Contemporary Mathematics **66**. American Mathematical Society, Providence, 1987.

[147] N. Gupta and V. Shpilrain, *Nielsen's commutator test for two-generator groups*. Math. Proc. Cambridge Philos. Soc. **114** (1993), 295–301.

[148] J. Gwozdziewicz, *Injectivity on one line*. Bull. Soc. Sci. Lett. Lodz Ser. Rech. Deform. **15** (1993), 59–60.

[149] O. Hadas, *On the vertices of Newton polytopes associated with an automorphism of the ring of polynomials*. J. Pure Appl. Algebra **76** (1991), 81–86.

[150] M. C. Hedges, *The Freiheitssatz for graded algebras*. J. London Math. Soc. **35** (1987), no. 2, 395–405.

[151] P. Hill and S. Pride, *Commutators, generators and conjugacy equations in groups*. Arch. Math. (Basel) **44** (1985), 1–14.

[152] W. Imrich and E. C. Turner, *Endomorphisms of free groups and their fixed points*. Math. Proc. Cambridge Philos. Soc. **105** (1989), 421–422.

[153] S. V. Ivanov, *On certain elements of free groups*. J. Algebra **204** (1998), 394–405.

[154] S. V. Ivanov, *On endomorphisms of free groups that preserve primitivity*. Arch. Math. (Basel) **72** (1999), 92–100.

[155] N. K. Iyudu, *Subalgebra membership problem and subalgebra standard basis*. In: *Algebra*. De Gruyter, Berlin, 2000, 137–143.

[156] N. Jacobson, *Restricted Lie algebras of characteristic p*. Trans. Amer. Math. Soc. **50** (1941), 15–25.

[157] N. Jacobson, *Structure and Representation of Jordan Algebras*. American Mathematical Society Colloquium Publication **39**. American Mathematical Society, Providence, 1968.

[158] Z. Jelonek, *The extension of regular and rational embeddings*. Math. Ann. **277** (1987), 113–120.

[159] Z. Jelonek, *Identity sets for polynomial automorphisms*. J. Pure Appl. Algebra **76** (1991), 333–337.

[160] Z. Jelonek, *A hypersurface which has the Abhyankar–Moh property*. Math. Ann. **308** (1997), 73–84.

[161] Z. Jelonek, *A solution of the problem of van den Essen and Shpilrain*. J. Pure Appl. Algebra **137** (1999), 49–55.

[162] Z. Jelonek, *Testing sets for properness of polynomial mappings*. Math. Ann. **315** (1999), 1–35.

[163] Z. Jelonek, *Test polynomials*. J. Pure Appl. Algebra **147** (2000), 125–132.

[164] H. W. E. Jung, *Über ganze birationale Transformationen der Ebene*. J. Reine Angew. Math. **184** (1942), 161–174.

[165] R. N. Kalia and G. Rosenberger, *Automorphisms of the Fuchsian groups of type* $(0, 2, 2, 2, q : 0)$. Commun. Algebra **6** (1978), 1115–1129.

[166] S. Kaliman, *Extensions of isomorphisms between affine algebraic subvarieties of k^n to automorphisms of k^n*. Proc. Amer. Math. Soc. **113** (1991), 325–334.

[167] S. Kaliman, *On the Jacobian conjecture*. Proc. Amer. Math. Soc. **117** (1993), 45–51.

[168] S. Kaliman, *Smooth contractible hypersurfaces in $\mathbb{C}^n$ and exotic algebraic structures on $\mathbb{C}^3$*. Math. Z. **214** (1993), 499–510.

[169] S. Kaliman, *Polynomials with general $\mathbb{C}^2$-fibers are variables*. Preprint.

[170] S. Kaliman and M. Zaidenberg, *Affine modifications and affine varieties with a very transitive automorphism group*. Transform. Groups **4** (1999), 53–95.

[171] S. Kaliman and M. Zaidenberg, *Families of affine planes: the existence of a cylinder*, Michigan Math. J. **49** (2001), 353–367.

[172] I. Kapovich, P. Schupp, and V. Shpilrain, *Generic properties of the Whitehead algorithm, stabilizers in* $\mathrm{Aut}(F_k)$ *and one-relator groups*, preprint.

[173] O. Keller, *Ganze Cremona-Transformationen*. Monatsh. Math. Phys. **47** (1939), 299–306.

[174] A. R. Kemer, *Capelli identities and nilpotency of the radical of finitely generated PI-algebras*. Dokl. Akad. Nauk SSSR **255** (1980), 793–796. English translation: Sov. Math. Dokl. **22** (1980), 750–753.

[175] O. G. Kharlampovich, *Lyndon condition for solvable Lie algebras*. Izv. Vyssh. Uchebn. Zaved. Mat. **9** (1984), no. 9, 50–59. English translation: Sov. Math. (Iz. VUZ) **28** (1984), no. 9, 67–80.

[176] O. Kharlampovich and A. G. Myasnikov, *Irreducible affine varieties over a free group. I. Irreducibility of quadratic equations and Nullstellensatz*. J. Algebra **200** (1998), 472–516.

[177] O. Kharlampovich and A. G. Myasnikov, *Irreducible affine varieties over a free group. II. Systems in triangular quasi-quadratic form and description of residually free groups*. J. Algebra **200** (1998), 517–570.

[178] O. G. Kharlampovich and M. V. Sapir, *Algorithmic problems in varieties*. Internat. J. Algebra Comput. **5** (1995), 379–602.

[179] D. G. Khramtsov, *Finite groups of automorphisms of free groups*. Mat. Zametki **38** (1985), no. 3, 386–392. English translation: Math. Notes **38** (1985), 721–724.

[180] E. Kiral and N. Ekici, *Recognizing automorphisms of the free color Lie superalgebras*. J. Algebra and Its Applications **1** (2002), no. 3, 335–340.

[181] A. T. Kolotov, *Free subalgebras of free associative algebras*. Sibirsk. Mat. Zh. **19** (1978), no. 2, 328–335, 478. English translation: Siberian Math. J. **19** (1978), no. 2, 229–234.

[182] J. Konieczny, G. Rosenberger, and J. Wolny, *Tame almost primitive elements*. Results Math. **38** (2000), 116–129.

[183] J. Kowalski, G. Rosenberger, and J. Wolny, *On equations in the free group of rank 2 and the classification of almost primitive elements.* In: A. C. Kim (ed.), *Groups–Korea'98 (Pusan).* De Gruyter, Berlin, 2000, 229–241.

[184] H. Kraft, *On a question of Yosef Stein.* In: A. van den Essen (ed.), *Automorphisms of affine spaces (Curacao, 1994).* Kluwer Academic Publishers, Dordrecht, 1995, 225–229.

[185] H. Kraft, *Challenging problems on affine n-space.* Astérisque **237** (1996), 295–317.

[186] A. F. Krasnikov, *Generating elements of the group $F/[N,N]$.* Mat. Zametki **24** (1978), no. 2, 167–173. English translation: Math. Notes **24** (1978), 591–594.

[187] P. Kropholler, P. Linnell, and J. Moody, *Applications of a new K-theoretic theorem to solvable group rings.* Proc. Amer. Math. Soc. **194** (1988), 675–684.

[188] G. V. Kryazhovskih, *Approximability of finitely presented algebras.* Sibirsk. Mat. Zh. **21** (1980), no. 5, 58–62. English translation: Siberian Math. J. **21** (1980), 688–691.

[189] G. V. Kryazhovskih, *Generating and defining relations of subalgebras of Lie algebras.* Sibirsk. Mat. Zh. **24** (1983), no. 6, 80–86. English translation: Siberian Math. J. **24** (1983), 889–894.

[190] G. V. Kryazhovskih and G. P. Kukin, *On subrings of free rings.* Sibirsk. Mat. Zh. **30** (1989), no. 6, 87–97. English translation: Siberian Math. J. **30** (1989), 903–914.

[191] G. P. Kukin, *Primitive elements of free Lie algebras.* Algebra i Logika **9** (1970), no. 4, 458–472. English translation: Algebra and Logic **9** (1970), 275–284.

[192] G. P. Kukin, *On subalgebras of free Lie p-algebras.* Algebra i Logika **11** (1972), 535–550. English translation: Algebra and Logic **11** (1972), 33–50.

[193] G. P. Kukin, *The word problem and free products of Lie algebras and associative algebras.* Sibirsk. Mat. Zh. **24** (1983), no. 2, 85–96. English translation: Siberian Math. J. **24** (1983), 221–231.

[194] W. van der Kulk, *On polynomial rings in two variables.* Nieuw Archief voor Wiskunde **1** (1953), no. 3, 33–41.

[195] A. G. Kurosh, *Non-associative free algebras and free products of algebras.* Mat. Sb. **20** (1947), 239–262.

[196] A. G. Kurosh, *Nonassociative free sums of algebras.* Mat. Sb. **37** (1955), no. 2, 251–264.

[197] A. G. Kurosh, *Free sums of multioperator algebras.* Sibirsk. Mat. Zh. **1** (1960), no. 1, 62–70; corrections — Sibirsk. Mat. Zh. **1** (1960), no. 4, 638.

[198] A. G. Kurosh, *The Theory of Groups, 2nd English Ed.* Chelsea Publishing Company, New York, 1960.

[199] A. G. Kurosh, *Lectures in General Algebra.* Pergamon Press, Oxford, 1965.

[200] C.-M. Lam and J.-T. Yu, *Tame and wild coordinates of $\mathbb{Z}[x,y]$.* J. Algebra, to appear.

[201] J. Lang, *Newton polygons of Jacobian pairs.* J. Pure Appl. Algebra **72** (1991), 39–51.

[202] M. Lazard, *Groupes, Anneaux de Lie et Problème de Burnside.* Instituto Matematica dell' Universita Roma, Roma, 1960.

[203] L. Le Bruyn, *Automorphisms and Lie stacks.* Commun. Algebra **25** (1997), 2211–2226.

[204] D. Lee, *On certain C-test words for free groups.* J. Algebra **247** (2002), 509–540.

[205] D. Lee, *Primitivity preserving endomorphisms of free groups.* Commun. Algebra **30** (2002), 1921–1947.

[206] D. Lee, *Endomorphisms of free groups that preserve automorphic orbits.* J. Algebra **248** (2002), 230–236.

[207] D. Lee, *Counting words of minimum length in an automorphic orbit,* preprint.

[208] W. Lee, *Wild automorphisms of generic matrix algebras.* J. Pure Appl. Algebra **148** (2000), 267–270.

[209] J. Lepowsky and R. L. Wilson, *On Hopf algebras and the elimination theorem for free Lie algebras.* Contemporary Mathematics **193**. American Mathematical Society, Providence, 1996, 191–202.

[210] G. Levitt and J.-L. Nicolas, *On the maximum order of torsion elements in* $\mathrm{GL}(n, Z)$ *and* $\mathrm{Aut}(F_n)$. J. Algebra **208** (1998), 630–642.

[211] G. Levitt and M. Lustig, *Periodic ends, growth rates, Hölder dynamics for automorphisms of free groups.* Comment. Math. Helv. **75** (2000), 415–429.

[212] J. Lewin, *On Schreier varieties of linear algebras.* Trans. Amer. Math. Soc. **132** (1968), 553–562.

[213] J. Lewin, *Free modules over free algebras and free group algebras: the Schreier technique.* Trans. Amer. Math. Soc. **145** (1969), 455–465.

[214] J. Lewin, *A note on zero divisors in group rings.* Proc. Amer. Math. Soc. **31** (1972), 357–359.

[215] J. Lewin and T. Lewin, *On ideals of free associative algebras generated by a single element.* J. Algebra **8** (1968), 248–255.

[216] W. Li, *On a problem about face polynomials.* J. Pure Appl. Algebra **60** (1989), 269–272.

[217] W. Li and J.-T. Yu, *Reconstructing birational maps from their face functions.* Manuscripta Math. **76** (1992), 353–366.

[218] W. Li and J.-T. Yu, *Computing minimal polynomials and the degree of unfaithfulness.* Commun. Algebra **21** (1993), 3557–3569.

[219] A. I. Lichtman and M. Shirvani, *HNN-extensions of Lie algebras.* Proc. Amer. Math. Soc. **125** (1997), 3501–3508.

[220] V. Ya. Lin and M. G. Zaidenberg, *An irreducible, simply connected algebraic curve in* $\mathbb{C}^2$ *is equivalent to a quasihomogeneous curve.* Dokl. Akad. Nauk SSSR **271** (1983), 1048–1052. English translation: Soviet Math. Dokl. **28** (1983), 200–204.

[221] J.-L. Loday, *Cyclic homology and the Lie algebra homology of matrices.* Comment. Math. Helw. **59** (1984), 569–591.

[222] J.-L. Loday, *Une version non commutative des algèbres de Lie: les algèbres de Leibniz.* L'Enseignement Math. **39** (1993), 269–293.

[223] J.-L. Loday and T. Pirashvili, *Universal enveloping algebras of Leibniz algebras and (co)homology.* Math. Ann. **296** (1993), 139–158.

[224] A. Logar and B. Sturmfels, *Algorithms for the Quillen–Suslin theorem.* J. Algebra **145** (1992), 231–239.

[225] R. C. Lyndon, *The equation $a^2b^2 = c^2$ in free groups.* Michigan Math. J. **6** (1959), 89–95.

[226] R. C. Lyndon, *Equations in groups.* Bol. Soc. Brasil. Mat. **11** (1980), 79–102.

[227] R. Lyndon and P. Schupp, *Combinatorial Group Theory.* Reprint of the 1977 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2001.

[228] R. C. Lyndon and M. P. Schützenberger, *The equation $a^M = b^N c^P$ in a free group.* Michigan Math. J. **9** (1962), 289–298.

[229] W. Magnus, *Über diskontinuierliche Gruppen mit einer definierden Relation (Der Freiheitssatz).* J. Reine Angew. Math. **163** (1930), 141–165.

[230] W. Magnus, *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring.* Math. Ann. **111** (1935), 259–280.

[231] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial Group Theory, 2nd Ed.* Dover, New York, 1976.

[232] G. S. Makanin, *Equations in a free group.* Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), 1199–1273. English translation: Math. USSR-Izv. **21** (1983), 546–582.

[233] L. G. Makar-Limanov, *On automorphisms of free algebra with two generators.* Funk. Analiz Prilozh. **4** (1970), no. 3, 107–108. English translation: Funct. Anal. Appl. **4** (1970), 262–264.

[234] L. G. Makar-Limanov, *Algebraically closed skew fields.* J. Algebra **93** (1985), 117–135.

[235] L. Makar-Limanov, *On the hypersurface $x + x^2y + z^2 + t^3 = 0$ in $\mathbb{C}^4$ or a $\mathbb{C}^3$-like threefold which is not $\mathbb{C}^3$.* Israel J. Math. **96** (1996), 419–429.

[236] L. Makar-Limanov, P. van Rossum, V. Shpilrain, and J.-T. Yu, *The stable equivalence and cancellation problems*, preprint.

[237] A. I. Malcev, *On algebras defined by identities.* Mat. Sb. **26** (1950), 19–33.

[238] A. I. Malcev, *Algebraic Systems.* Springer-Verlag, Berlin, 1973.

[239] H. Matsumura, *Commutative Algebra.* W. A. Benjamin, New York, 1970.

[240] J. McCool, *A characterization of periodic automorphisms of a free group.* Trans. Amer. Math. Soc. **260** (1980), 309–318.

[241] J. McCool and A. Pietrowski, *On free products with amalgamation of two infinite cyclic groups.* J. Algebra **18** (1971), 377–383.

[242] J. McKay and S. S. Wang, *An inversion formula for two polynomials in two variables.* J. Pure Appl. Algebra **40** (1986), 245–257.

[243] A. A. Mikhalev, *Subalgebras of free color Lie superalgebras.* Mat. Zametki **37** (1985), no. 5, 653–661. English translation: Math. Notes **37** (1985), 356–360.

[244] A. A. Mikhalev, *Free color Lie superalgebras.* Dokl. Akad. Nauk SSSR **286** (1986), no. 3, 551–554. English translation: Soviet Math. Dokl. **33** (1986), 136–139.

[245] A. A. Mikhalev, *Subalgebras of free Lie p-superalgebras.* Mat. Zametki **43** (1988), no. 2, 178–191. English translation: Math. Notes **43** (1988), 99–106.

[246] A. A. Mikhalev, *A composition lemma and the word problem for color Lie superalgebras.* Vestnik Moskov. Univ. Ser. I. Mat. Mekh. (1989), no. 5, 88–91. English translation: Moscow Univ. Math. Bull. **44** (1989), no. 5, 87–90.

[247] A. A. Mikhalev, *Ado–Iwasawa theorem, graded Hopf algebras and residual finiteness of color Lie (p-)superalgebras and their universal enveloping algebras.* Vestnik Moskov. Univ. Ser. I. Mat. Mekh. (1991), no. 5, 72–74. English translation: Moscow Univ. Math. Bull. **46** (1991), no. 5, 51–53.

[248] A. A. Mikhalev, *Free color Lie super-rings.* Izv. Vyssh. Uchebn. Zaved. Mat. (1991), no. 10, 46–49. English translation: Soviet Math. (Izv. VUZ) **35** (1991), no. 10, 42–44.

[249] A. A. Mikhalev, *On right ideals of the free associative algebra generated by free color Lie (p-)superalgebras.* Uspekhi Mat. Nauk **47** (1992), no. 5, 187–188. English translation: Russian Math. Surveys **47** (1992), no. 5, 196–197.

[250] A. A. Mikhalev, *The composition lemma for color Lie superalgebras and for Lie p-superalgebras.* Contemp. Math. **131** (1992), no. 2, 91–104.

[251] A. A. Mikhalev, *Shirshov composition techniques in Lie superalgebras (noncommutative Gröbner bases).* Trudy Semin. im. I. G. Petrovskogo **18** (1995), 277–289. English translation: J. Math. Sci. **80** (1996), no. 5, 2153–2160.

[252] A. A. Mikhalev, *Combinatorial aspects of the theory of Lie superalgebras.* In: *First International Tainan–Moscow Algebra Workshop.* Walter de Gruyter, Berlin, 1996, 37–68.

[253] A. A. Mikhalev, *Primitive elements and automorphisms of free algebras of Schreier varieties.* J. Math. Sci. **102** (2000), no. 6, 4628–4640.

[254] A. A. Mikhalev, V. Shpilrain, and U. U. Umirbaev, *On isomorphism of Lie algebras with one defining relation.* Intern. J. Algebra Comput., to appear.

[255] A. A. Mikhalev, V. Shpilrain, and J.-T. Yu, *On endomorphisms of free algebras.* Algebra Colloq. **6** (1999), 241–248.

[256] A. A. Mikhalev, V. Shpilrain, and J.-T. Yu, *Combinatorial problems about free groups and algebras.* In: *Lie Algebras, Rings and Related Topics.* Springer-Verlag, Hong Kong, 2000, 80–107.

[257] A. A. Mikhalev, V. Shpilrain, and A. A. Zolotykh, *Subalgebras of free algebras.* Proc. Amer. Math. Soc. **124** (1996), 1977–1983.

[258] A. A. Mikhalev and U. U. Umirbaev, *Subalgebras of free Leibniz algebras.* Commun. Algebra **26** (1998), 435–446.

[259] A. A. Mikhalev, U. U. Umirbaev, and J.-T. Yu, *Automorphic orbits of elements of free non-associative algebras.* J. Algebra **243** (2001), 198–223.

[260] A. A. Mikhalev, U. U. Umirbaev, and J.-T. Yu, *Generic, almost primitive and test elements of free Lie algebras.* Proc. Amer. Math. Soc. **130** (2002), 1303–1310.

[261] A. A. Mikhalev, U. U. Umirbaev, and A. A. Zolotykh, *An example of a nonfree Lie algebra of cohomological dimension one.* Uspekhi Mat. Nauk **49** (1994), no. 1, 203–204. English translation: Russian Math. Surveys **49** (1994), no. 1, p. 254.

[262] A. A. Mikhalev, U. U. Umirbaev, and A. A. Zolotykh, *A Lie algebra with cohomological dimension one over a field of prime characteristic is not necessarily free.* In: Y. Fong, U. Knauer, and A. Mikhalev (eds.), *First International Tainan-Moscow Algebra Workshop.* Walter de Gruyter, Berlin, 1996, 257–264.

[263] A. A. Mikhalev and J.-T. Yu, *Test elements and retracts of free Lie algebras.* Commun. Algebra **25** (1997), 3283–3289.

[264] A. A. Mikhalev and J.-T. Yu, *Test elements, retracts and automorphic orbits of free algebras*, Intern. J. Algebra Comput. **8** (1998), 295–310.

[265] A. A. Mikhalev and J.-T. Yu, *Primitive, almost primitive, test, and Δ-primitive elements of free algebras with the Nielsen–Schreier property.* J. Algebra **228** (2000), 603–623.

[266] A. A. Mikhalev and J.-T. Yu, *Automorphic orbits of elements of free algebras with the Nielsen–Schreier property.* Contemporary Mathematics **264**. American Mathematical Society, Providence, 2000, 95–110.

[267] A. A. Mikhalev and J.-T. Yu, *Stable equivalence problems for free algebras with the Nielsen–Schreier property.* Intern. J. Algebra Comput. **11** (2001), 779–786.

[268] A. A. Mikhalev, J.-T. Yu, and A. A. Zolotykh, *Images of coordinate polynomials.* Algebra Colloq. **4** (1997), 159–162.

[269] A. A. Mikhalev and A. A. Zolotykh, *Endomorphisms of free Lie algebras preserving primitivity of elements are automorphisms*. Uspekhi Mat. Nauk **48** (1993), no. 6, 149–150. English translation: Russian Math. Surveys **48** (1993), no. 6, 189–190.

[270] A. A. Mikhalev and A. A. Zolotykh, *Applications of Fox differential calculus to free Lie superalgebras.* In: *Non-Associative Algebra and Its Applications.* Kluwer Academic Publishers, Dordrecht, 1994, 285–290.

[271] A. A. Mikhalev and A. A. Zolotykh, *Automorphisms and primitive elements of free Lie superalgebras.* Commun. Algebra **22** (1994), 5889–5901.

[272] A. A. Mikhalev and A. A. Zolotykh, *Rank and primitivity of elements of free color Lie (p-)superalgebras.* Intern. J. Algebra Comput. **4** (1994), 617–656.

[273] A. A. Mikhalev and A. A. Zolotykh, *The rank of an element of the free color Lie (p-)superalgebra.* Dokl. Akad. Nauk **334** (1994), 690–693. English translation: Russian Acad. Sci. Dokl. Math. **49** (1994), no. 1, 189–193.

[274] A. A. Mikhalev and A. A. Zolotykh, *An inverse function theorem for free Lie algebras over commutative rings.* Algebra Colloq. **2** (1995), 213–220.

[275] A. A. Mikhalev and A. A. Zolotykh, *Combinatorial Aspects of Lie Superalgebras.* CRC Press, Boca Raton/New York, 1995.

[276] A. A. Mikhalev and A. A. Zolotykh, *Endomorphisms of free associative algebras over commutative rings and their Jacobian matrices.* Fundam. Prikl. Mat. **1** (1995), 177–190.

[277] A. A. Mikhalev and A. A. Zolotykh, *Test elements for monomorphisms of free Lie algebras and Lie superalgebras.* Commun. Algebra **23** (1995), 4995–5001.

[278] A. A. Mikhalev and A. A. Zolotykh, *Algorithms for primitive elements of free Lie algebras and superalgebras.* In: Y. N. Lakshman (ed.), *Proceedings of ISSAC-96.* ACM Press, New York, 1996, 161–169.

[279] A. A. Mikhalev and A. A. Zolotykh, *Ranks of subalgebras of free Lie superalgebras.* Vestnik Moskov. Univ. Ser. I. Mat. Mekh. (1996), no. 2, 36–40. English translation: Moscow Univ. Math. Bull. **51** (1996), no. 2, 32–35.

[280] A. A. Mikhalev and A. A. Zolotykh, *A complex of algorithms for computations in Lie superalgebras.* Programmirovanie (1997), no. 1, 12–23. English translation: Program. Comput. Software **23** (1997), no. 1, 8–16.

[281] M. Miyanishi, *Some remarks on polynomial rings.* Osaka J. Math. **10** (1973), 617–624.

[282] M. Miyanishi and T. Sugie, *Affine surfaces containing cylinderlike open sets.* J. Math. Kyoto Univ. **20** (1980), 11–42.

[283] T. T. Moh, *On the Jacobian conjecture and the configurations of roots.* J. Reine Angew. Math. **340** (1983), 140–212.

[284] D. Mumford, *Algebraic Geometry I. Complex Projective Varieties.* Springer-Verlag, Berlin, 1976.

[285] A. G. Myasnikov and V. Remeslennikov, *Algebraic geometry over groups. II. Logical foundations.* J. Algebra **234** (2000), 225–276.

[286] A. G. Myasnikov and V. Shpilrain, *Automorphic orbits in free groups.* J. Algebra, to appear.

[287] H. Nagao, *On* $\mathrm{GL}(2, K[x])$. J. Inst. Polytech. Osaka City Univ. Ser. A **10** (1959), 117–121.

[288] M. Nagata, *On the Automorphism Group of* $k[x, y]$. Lectures in Mathematics, Kyoto University. Kinokuniya, Tokyo, 1972.

[289] J. O'Neill and E. Turner, *Test elements and the retract theorem in hyperbolic groups.* New York J. Math. **6** (2000), 107–117 (electronic).

[290] J. O'Neill and E. Turner, *Test elements in direct products of groups.* Intern. J. Algebra Comput. **10** (2000), 751–756.

[291] H. Neumann, *Varieties of Groups.* Springer-Verlag, Berlin, 1967.

[292] W. Neumann and P. Wightwick, *Algorithms for polynomials in two variables.* In: *Combinatorial and computational algebra (Hong Kong, 1999).* Contemporary Mathematics **264**. American Mathematical Society, Providence, 2000, 219–235.

[293] J. Nielsen, *Die Isomorphismen der allgemeinen, unendlichen Gruppe mit zwei Erzeugenden.* Math. Ann. **78** (1918), 385–397.

[294] J. Nielsen, *Die Isomorphismengruppe der freien Gruppe.* Math. Ann. **91** (1924), 169–209.

[295] A. Yu. Olshanskii, *Geometry of Defining Relations in Groups.* Mathematics and Its Applications (Soviet Series) **70**. Kluwer Academic Publishers, Dordrecht, 1991.

[296] R. P. Osborne and H. Zieschang, *Primitives in the free group on two generators.* Invent. Math. **63** (1981), 17–24.

[297] H. Park, *A Computational Theory of Laurent Polynomial Rings and Multidimensional FIR Systems.* Ph. D. Thesis, University of California, Berkeley, 1995.

[298] H. Park, *A realization algorithm for* $\mathrm{SL}_2(k[x_1, \ldots, x_m])$ *over the Euclidean domain.* SIAM J. Matrix Anal. Appl. **21** (1999), 178–184 (electronic).

[299] H. Park and C. Woodburn, *An algorithmic proof of Suslin's stability theorem for polynomial rings.* J. Algebra **178** (1995), 277–298.

[300] D. S. Passman, *The Algebraic Structure of Group Rings.* John Wiley and Sons, New York, 1977.

[301] P. Pedersen and B. Sturmfels, *Product formulas for resultants and Chow forms.* Math. Z. **214** (1993), 377–396.

[302] V. M. Petrogradsky, *Exponential Schreier's formula for free Lie algebras and its applications.* J. Math. Sci. **93** (1999), no. 6, 939–950.

[303] V. M. Petrogradsky, *Schreier's formula for free Lie algebras.* Arch. Math. (Basel) **75** (2000), 16–28.

[304] V. M. Petrogradsky, *Schreier's formula for free Lie algebras, their applications and asymptotics.* In: *Algebra (Moscow, 1998).* De Gruyter, Berlin, 2000, 281–289.

[305] V. M. Petrogradsky, *On generating functions for subalgebras of free Lie superalgebras.* Discrete Math. **246** (2002), 269–284.

[306] V. M. Petrogradsky, *Schreier's formulas for varieties of algebras and their applications.* Preprint.

[307] B. Plotkin, *Varieties of algebras and algebraic varieties.* Israel J. Math. **96** (1996), part B, 511–522.

[308] B. Plotkin, *Some concepts of algebraic geometry in universal algebra.* Algebra Analiz **9** (1997), 224–248. English translation: St. Petersburg Math. J. **9** (1998), 859–879.

[309] P. Rabier, *On components of polynomial automorphisms in two variables.* Commun. Algebra **24** (1996), 929–937.

[310] Yu. P. Razmyslov, *The Jacobson radical in PI algebras.* Algebra i Logika **13** (1974), 337–360. English translation: Algebra and Logic **13** (1974), 192–204.

[311] Yu. P. Razmyslov, *Identities of Algebras and Their Representations.* American Mathematical Society, Providence, 1994.

[312] C. Reutenauer, *Applications of a noncommutative Jacobian matrix.* J. Pure Appl. Algebra **77** (1992), 169–181.

[313] C. Reutenauer, *Free Lie Algebras.* Clarendon Press, Oxford, 1993.

[314] E. Rips, *Commutator equations in free groups*, Israel J. Math. **39** (1981), 326–340.

[315] I. Rivin, *A remark on "Counting primitive elements in free groups" (by J. Burillo and E. Ventura)*, preprint.

[316] C. F. Rocca Jr. and E. C. Turner, *Test ranks of finitely generated abelian groups*. Contemporary Mathematics **296**. American Mathematical Society, Providence, 2002, 199–206.

[317] V. A. Roman'kov, *Test elements for free solvable groups of rank* 2. Algebra i Logika **40** (2001), 192–201. English translation: Algebra and Logic **40** (2001), 106–111.

[318] G. Rosenberger, *Alternierende Produkte in freien Gruppen*, Pacific J. Math. **78** (1978), 243–250.

[319] G. Rosenberger, *Über Darstellungen von Elementen und Untergruppen in freien Produkten*. In: A. C. Kim and B. H. Neumann (eds.), *Groups–Korea 1983 (Kyoungju, 1983)*, Lecture Notes in Mathematics **1098**. Springer, Berlin, 1984, 142–160.

[320] G. Rosenberger, *Minimal generating systems for plane discontinuous groups and an equation in free groups*. Lecture Notes in Mathematics **1398**. Springer, Berlin, 1989, 170–186.

[321] G. Rosenberger, *A property of subgroups of free groups*. Bull. Austral. Math. Soc. **43** (1991), 269–272.

[322] S. Rosset and A. Wasserman, *The Schreier technique for subalgebras of a free Lie algebra*. Can. J. Math. **49** (1997), 600–616.

[323] L. H. Rowen, *Polynomial Identities in Ring Theory*. Academic Press, New York, 1980.

[324] P. Russell and A. Sathaye, *On finding and cancelling variables in* $k[X, Y, Z]$. J. Algebra **57** (1979), 151–166.

[325] A. Sathaye, *On linear planes*. Proc. Amer. Math. Soc. **56** (1976), 1–7.

[326] M. Scheunert, *Generalized Lie algebras*. J. Math. Phys. **20** (1979), 712–720.

[327] M. Scheunert, *The Theory of Lie Superalgebras. An Introduction*. Lecture Notes in Mathematics **716**. Springer, Berlin, 1979.

[328] A. H. Schofield, *Representations of Rings over Skew Fields*. Cambridge University Press, Cambridge, 1985.

[329] O. Schreier, *Die Untergruppen der freien Gruppen*. Abh. Math. Semin. Univ. Hamburg **5** (1927), 161–183.

[330] B. Segre, *Forme Differenziali e Loro Integrali, vol. II*. Docet, Roma, 1956.

[331] B. Segre, *Corrispondenze di Mobius e transformazioni cremoniane intere*. Atti della Accademia Scienze di Torino, Classer di Scienzo Fissiche, Mat. Natural. **91** (1956–1957), 3–19.

[332] B. Segre, *Variazione continua ed omotopia in geometria algebrica*. Ann. Mat. Pura Appl. (4) **50** (1960), 149–186.

[333] A. V. Sereguine, *Some properties of Lie algebras of cohomological dimension one*. Fundam. Prikl. Mat. **4** (1998), 779–783.

[334] I. R. Shafarevich, *On some infinite-dimensional groups.* Rend. Mat. Appl. **25** (1966), 208–212.

[335] D. Shannon and M. Sweedler, *Using Gröbner bases to determine membership, split surjective algebra homomorphisms birational equivalence.* J. Symbolic Comput. **6** (1988), 267–273.

[336] A. Shastri, *Polynomial representations of knots.* Tohoku Math. J. **44** (1992), no. 2, 11–17.

[337] I. P. Shestakov, A. I. Shirshov, A. M. Slinko, and K. A. Zhevlakov, *Rings that Are Nearly Associative.* Academic Press, New York, 1982.

[338] I. P. Shestakov and U. U. Umirbaev, *Free Akivis algebras, primitive elements, and hyperalgebras.* J. Algebra **250** (2002), 533–548.

[339] I. P. Shestakov and U. U. Umirbaev, *Poisson brackets and two-generated subalgebras of rings of polynomials.* Preprint, Sao Paulo, USP, 2002, 1–19.

[340] I. P. Shestakov and U. U. Umirbaev, *Tame and wild automorphisms of polynomial rings in three variables.* Preprint, Sao Paulo, USP, 2002, 1–34.

[341] I. P. Shestakov and U. U. Umirbaev, *Subalgebras and automorphisms of rings of polynomials.* Doklady Akad. Nauk **386** (2002), no. 6, 745–748. English translation: Russian Acad. Sci. Dokl. Math.

[342] I. P. Shestakov and U. U. Umirbaev, *Poisson brackets and two-generated subalgebras of rings of polynomials.* J. Amer. Math. Soc., to appear.

[343] I. P. Shestakov and U. U. Umirbaev, *Tame and wild automorphisms of rings of polynomials in three variables.* J. Amer. Math. Soc., to appear.

[344] I. P. Shestakov and U. U. Umirbaev, *The Nagata automorphism is wild.* Proc. Nat. Acad. Sci. USA, to appear.

[345] A. I. Shirshov, *Subalgebras of free Lie algebras.* Mat. Sb. **33** (1953), 441–452.

[346] A. I. Shirshov, *Subalgebras of free commutative and free anti-commutative algebras.* Mat. Sb. **34** (1954), 81–88.

[347] A. I. Shirshov, *Some algorithmical problems for ε-algebras.* Sibirsk. Mat. Zh. **3** (1962), 132–137.

[348] A. I. Shirshov, *Some algorithmical problems for Lie algebras.* Sibirsk. Mat. Zh. **3** (1962), 292–296.

[349] A. I. Shirshov, *Selected Works: Rings and Algebras.* Nauka, Moscow, 1984.

[350] V. Shpilrain, *An inverse function theorem for free associative algebras of rank two.* J. Pure Appl. Algebra **83** (1992), 23–26.

[351] V. Shpilrain, *On generators of L/R^2 Lie algebras.* Proc. Amer. Math. Soc. **119** (1993), 1039–1043.

[352] V. Shpilrain, *Recognizing automorphisms of the free groups.* Arch. Math. **62** (1994), 385–392.

[353] V. Shpilrain, *On monomorphisms of free groups.* Arch. Math. (Basel) **64** (1995), 465–470.

[354] V. Shpilrain, *On the rank of an element of a free Lie algebra.* Proc. Amer. Math. Soc. **123** (1995), 1303–1307.

[355] V. Shpilrain, *Test elements for endomorphisms of free groups and algebras.* Israel J. Math. **92** (1995), 307–316.

[356] V. Shpilrain, *Generalized primitive elements of a free group.* Arch. Math. (Basel) **71** (1998), 270–278.

[357] V. Shpilrain, *Combinatorial methods: from groups to polynomial algebras.* In: *Groups'97 Bath/St. Andrews, Vol. 2 (Bath, 1997)*, London Mathematical Society Lecture Note Series **261**, Cambridge University Press, Cambridge, 1999, 679–688.

[358] V. Shpilrain, *Counting primitive elements of a free group*, preprint.

[359] V. Shpilrain and J.-T. Yu, *Polynomial automorphisms and Gröbner reductions.* J. Algebra **197** (1997), 546–558.

[360] V. Shpilrain and J.-T. Yu, *On generators of polynomial algebras in two commuting or non-commuting variables.* J. Pure Appl. Algebra **132** (1998), 309–315.

[361] V. Shpilrain and J.-T. Yu, *Embeddings of curves in the plane.* J. Algebra **217** (1999), 668–678.

[362] V. Shpilrain and J.-T. Yu, *Peak reduction technique in commutative algebra: a survey.* In: *Combinatorial and Computational Algebra (Hong Kong, 1999)*, Contemporary Mathematics **264**. American Mathematical Society, Providence, 2000, 237–247.

[363] V. Shpilrain and J.-T. Yu, *Polynomial retracts and the Jacobian conjecture.* Trans. Amer. Math. Soc. **352** (2000), 477–484.

[364] V. Shpilrain and J.-T. Yu, *Embeddings of hypersurfaces in affine spaces.* J. Algebra **239** (2001), 161–173.

[365] V. Shpilrain and J.-T. Yu, *Affine varieties with equivalent cylinders.* J. Algebra **251** (2002), 295–307.

[366] V. Shpilrain and J.-T. Yu, *Non-extendable isomorphisms between affine varieties.* J. Pure Appl. Algebra **172** (2002), 285–291.

[367] V. Shpilrain and J.-T. Yu, *Some special factor algebras of free algebras.* Preprint.

[368] V. Shpilrain and J.-T. Yu, *Factor algebras of free algebras: on a problem of G. Bergman.* Bull. London Math. Soc. (2003).

[369] A. S. Shtern, *Free Lie superalgebras.* Sibirsk. Mat. Zh. **27** (1986), 170–174. English translation: Siberian Math. J. **27** (1986), 136–140.

[370] M. K. Smith, *Stably tame automorphisms.* J. Pure Appl. Algebra **58** (1989), 209–212.

[371] V. Srinivas, *On the embedding dimension of the affine variety.* Math. Ann. **289** (1991), 125–132.

[372] J. Stallings, *On torsion-free groups with infinitely many ends.* Ann. Math. **88** (1968), 312–334.

[373] J. R. Stallings, *Topology of finite graphs.* Invent. Math. **71** (1983), no. 3, 551–565.

[374] J. Stallings, *Generic elements in certain groups.* In: *Groups–Korea'94 (Pusan).* Walter de Gruyter, Berlin, 1995, 289–294.

[375] J. R. Stallings, *Problems about free quotients of groups.* In: *Geometric group theory (Columbus, OH, 1992)*, Ohio State University Mathematical Research Institute Publication **3**. De Gruyter, Berlin, 1995, 165–182.

[376] B. Sturmfels, *Sparse elimination theory.* In: *Proceedings of Computational Algebraic Geometry and Commutative Algebra, Ravello, Italy, June 8–13, 1992.* Cortona, Italy, 1993.

[377] B. Sturmfels and J.-T. Yu, *Minimal polynomials and sparse resultants.* In: *Proceedings of the Zero-Dimensional Conference at Ravello, Italy, June 8–13, 1992.* Cortona, Italy, 1993.

[378] A. A. Suslin, *Projective modules over polynomial rings are free.* Dokl. Akad. Nauk SSSR **229** (1976), 1063–1066. English translation: Soviet Math. Dokl. **17** (1976), 1160–1164.

[379] A. A. Suslin, *The structure of the special linear group over rings of polynomials.* Izv. Akad. Nauk SSSR. Ser. Mat. **41** (1977), no. 2, 235–252, 477. English translation: Math. USSR Izv. **11** (1977), 221–239.

[380] M. Suzuki, *Propriétés topologiques des polynomes de deux variables complexes, et automorphismes algébriques de l'espace* $\mathbb{C}^2$. J. Math. Soc. Japan **26** (1974), 241–257.

[381] R. G. Swan, *Groups of cohomological dimension one.* J. Algebra **12** (1969), 585–610.

[382] E. I. Timoshenko, *Test elements and test rank of a free metabelian group.* Sibirsk. Mat. Zh. **41** (2000), 1451–1456. English translation: Siberian Math. J. **41** (2000), 1200–1204.

[383] E. C. Turner, *Test words for automorphisms of free groups.* Bull. London Math. Soc. **28** (1996), no. 3, 255–263.

[384] V. A. Ufnarovskii, *Combinatorial and asymptotic methods in algebra.* In: *Itogi Nauki i Tekhniki, Sovremennye Problemy Matematiki. Fundamentalnye Napravleniya* **57**. VINITI, Moscow, 1990, 5–177. English translation: in *Algebra VI, Encyclopaedia of Math. Sci.* **57**, Springer, Berlin, 1995, 1–196.

[385] U. U. Umirbaev, *On the approximation of free Lie algebras with respect to entry.* Tartu Riikl. Ül. Toimetised **878** (1990), 147–152.

[386] U. U. Umirbaev, *Some algorithmic questions concerning associative algebras.* Algebra i Logika **32** (1993), no. 4, 450–470. English translation: Algebra and Logic **32** (1993), no. 4, 244–255.

[387] U. U. Umirbaev, *Partial derivatives and endomorphisms of some relatively free Lie algebras.* Sibirsk. Mat. Zh. **34** (1993), no. 6, 179–188. English translation: Siberian Math. J. **34** (1993), 1161–1170.

[388] U. U. Umirbaev, *On Schreier varieties of algebras.* Algebra i Logika **33** (1994), no. 3, 317–340. English translation: Algebra and Logic **33** (1994), no. 3, 180–193.

[389] U. U. Umirbaev, *Primitive elements of free groups.* Uspekhi Mat. Nauk **49** (1994), no. 2, 175–176. English translation: Russian Math. Surveys **49** (1994), no. 2, 184–185.

[390] U. U. Umirbaev, *On the extension of automorphisms of polynomial rings.* Sibirsk. Mat. Zh. **36** (1995), 911–916. English translation: Siberian Math. J. **36** (1995), 787–791.

[391] U. U. Umirbaev, *On ranks of elements of free groups.* Fundam. Prikl. Mat. **2** (1996), 313–315.

[392] U. U. Umirbaev, *Universal derivations and subalgebras of free algebras.* In: *Algebra (Krasnoyarsk, 1993).* Walter de Gruyter, Berlin, 1996, 255–271.

[393] U. U. Umirbaev and J.-T. Yu, *Strong Nagata conjecture.* Proc. Nat. Acad. Sci. USA, to appear.

[394] E. A. Vasilieva, *Endomorphisms of free supercommutative algebras.* Uspekhi Mat. Nauk **55** (2000), no. 1, 175–176. English translation: Russian Math. Surveys **55** (2000), no. 1, 190–191.

[395] G. Viennot, *Algèbres de Lie Libres et Monoïdes Libres.* Lecture Notes in Mathematics **691**. Springer, Berlin, 1978.

[396] D. Voce, *Test words of a free product of two finite cyclic groups.* Proc. Edinburgh Math. Soc. **40** (1997), no. 2, 551–562.

[397] S. S. Wang, *A Jacobian criterion for separability.* J. Algebra **65** (1980), 453–494.

[398] C. M. Weinbaum, *Partitioning a primitive word into a generating set.* Math. Ann. **18** (1969), 157–162.

[399] J. H. C. Whitehead, *On certain sets of elements in a free group.* Proc. London Math. Soc. **41** (1936), 48–56.

[400] J. H. C. Whitehead, *On equivalent sets of elements in a free group.* Ann. Math. **37** (1936), 782–800.

[401] P. Wightwick, *Equivalence of polynomials under automorphisms of* $\mathbb{C}^2$. J. Pure Appl. Algebra **157** (2001), 341–367.

[402] R. J. Wilson, *Introduction to Graph Theory.* Pearson, 1996.

[403] E. Witt, *Die Unterringe der freien Lieschen Ringe.* Math. Z. **64** (1956), 195–216.

[404] D. Wright, *The amalgamated free product structure of* $\mathrm{GL}_2(k[X_1, \ldots, X_n])$ *and the weak Jacobian theorem for two variables.* J. Pure Appl. Algebra **12** (1978), 235–251.

[405] D. Wright, *On the Jacobian conjecture.* Illinois J. Math. **25** (1981), 423–440.

[406] A. V. Yagzhev, *Endomorphisms of free algebras.* Sibirsk. Math. Zh. **21** (1980), 181–192. English translation: Siberian Math. J. **21** (1980), no. 1, 133–141.

[407] A. V. Yagzhev, *On the algorithmic problem of recognizing automorphisms among endomorphisms of free associative algebras of finite rank.* Sibirsk. Math. Zh. **21** (1980), 193–199. English translation: Siberian Math. J. **21** (1980), 142–146.

[408] A. V. Yagzhev, *Invertibility of endomorphisms of free associative algebras.* Mat. Zametki **49** (1991), no. 4, 142–147. English translation: Math. Notes **49** (1991), 426–430.

[409] J.-T. Yu, *Face polynomials and inversion formula.* J. Pure Appl. Algebra **78** (1992), 213–219.

[410] J.-T. Yu, *Computing minimal polynomials and the inverse via GCP.* Commun. Algebra **21** (1993), 2279–2294.

[411] J.-T. Yu, *A product formula for minimal polynomials and degree bounds for inverses of polynomial automorphisms.* Proc. Amer. Math. Soc. **123** (1995), 343–349.

[412] J.-T. Yu, *On the Jacobian conjecture: reduction of coefficients.* J. Algebra **171** (1995), 515–523.

[413] J.-T. Yu, *Identity polynomials and test polynomials.* Algebra Colloq. **4** (1997), 29–36.

[414] M. V. Zaicev, *Schreier varieties of Lie algebras.* Mat. Zametki **28** (1980), no. 1, 119–126. English translation: Math. Notes **28** (1980), nos. 1–2, 523–526.

[415] M. G. Zaidenberg, *On exotic algebraic structures on affine spaces.* In: *Geometric complex analysis (Hayama, 1995).* World Scientific Publishing, River Edge, NJ, 1996, 691–714.

[416] A. I. Zhukov, *Reduced systems of defining relations in non-associative algebras.* Mat. Sb. **27** (1950), 267–280.

[417] H. Zieschang, *Alternierende Produkte in freien Gruppen.* Abh. Math. Sem. Univ. Hamburg **27** (1964), 12–31.

[418] H. Zieschang, *Über Automorphismen ebener discontinuerlicher Gruppen.* Math. Ann. **166** (1966), 148–167.

[419] A. A. Zolotykh, *Commutation factors and varieties of associative algebras.* Fundam. Prikl. Mat. **3** (1997), 453–468.

Notation Index

$A(n, K)$, 92
$A(u)$, 46, 48
a°, 192
A^α, 225
$a_i = \frac{\partial a}{\partial x_i} = \frac{\partial}{\partial x_i} a$, 206
$\operatorname{ad} a$, 195
$\operatorname{Ad} b$, 195
$\operatorname{Ann}(A)$, 279
$\operatorname{Aut}(K[X])$, 92
$\operatorname{Aut}^\circ(A_2)$, 139
$\operatorname{Aut}^\circ(P_2)$, 139
$\operatorname{Aut}^0(R[x, y])$, 158
$\operatorname{Aut}_{IL}(A_2)$, 139
$\operatorname{Aut}_{IL}(P_2)$, 139
$\operatorname{Aut}^e_{IL}(A_2)$, 139
$\operatorname{Aut}^e_{IL}(P_2)$, 139

$\mathcal{D}\colon A \to I_A$, 201
$\partial(f)$, 202
$\frac{\partial f}{\partial x_i}$, 202
D_u, 33
Δ, 14, 262
Δ_R, 14

$\mathcal{E}\colon \mathbb{Z}_0[[t]] \to \mathbb{Z}[[t]]$, 200

$f^{(k)}$, 222
$F_{\mathfrak{M}}(X)$, 185
F_n, 8, 9
$\operatorname{Fix}(\varphi)$, 26

$\Gamma(X)$, 192
$\gamma_k(R)$, 14
$\mathrm{GE}_2(R[x, y])$, 150

$\mathcal{H}_X(V, t)$, 200
$\mathcal{H}_X(Y, t)$, 200

$J(n, K)$, 92
$J(\varphi)$, 105, 220
J_φ, 141
J_F, 149
J_H, 202, 273
$J_k(\varphi)$, 220, 231

K, 185
$K[p_1, \ldots, p_n]$, 67
$K[X]$, 122
$K\langle X\rangle$, 101
$K[x_1, \ldots, x_n]$, 67

$L(X)$, 195

$L^p(X)$, 195
L_X, 228
$LB\langle x_1, x_2\rangle$, 279

$\mathfrak{M}$, 185
$m(w)$, 217
$\mathfrak{M}_0$, 193
$\mathfrak{M}_1$, 193
$\mathfrak{M}_2$, 194
M_a, 225
$\mu(w)$, 217
$\mu\colon X \to \mathbb{N}$, 192
$\mu\colon \mathbb{Z}_+^n \to \mathbb{Q}_+$, 217
$\mu_1 \prec \mu_2$, 225

$\mathfrak{N}_m$, 269

$\mathrm{Orb}_{\mathrm{Aut}\, F_n}(u)$, 45
$\mathrm{Orb}(h)$, 245
$\mathrm{Orb}(u)$, 254, 255
$\mathrm{Orb}_\varphi(u)$, 46

$P(r, n)$, 48
p_x, 149
p_y, 149
φ_∞, 26
$\varphi^\infty(F)$, 26
$\Phi(m)$, 52

$[Q]$, 195
$[Q]^p$, 195
$\mathbb{Q}_+$, 217

R_+, 195
R_-, 195
$\mathrm{rank}(M)$, 198
$\mathrm{rank}(M_a)$, 225
$\mathrm{rank}(u)$, 208
$\rho_\mu^\alpha(f)$, 225

$T(n, K)$, 92

$U(L)$, 202
$u(L)$, 203
U^α, 225
$UL(A)$, 279
$UL(L)$, 272

$V(\mu)$, 225
$V(p_1, \ldots, p_m)$, 80

$\mathrm{Wh}(u)$, 49

X_+, 198
X_-, 198

$\mathbb{Z}_+$, 217
$\mathbb{Z}F$, 14

Author Index

Abdykhalykov A. T., 283
Abhyankar S. S., 68–71, 73, 75, 80, 81, 83, 84, 95, 98, 108, 110, 128, 236, 283, 284
Adams W. W., 284
Agalakov S. A., 237, 284
Akivis M. A., 206
Alev J., 284
Anick D. J., 145, 284
Appelgate H., 284
Artal-Bartolo E., 284
Artamonov V. A., 36, 107, 247, 284
Asanuma T., 285

Bachmuth S., 21, 23, 25, 285
Bahturin Yu. A., 191, 271, 285
Bandman T., 285
Baranovich T. M., 285
Bass H., 2, 72, 285
Baumslag G., vii, 3, 285
Bencsath K., 285
Bergman G. M., 127, 130, 254, 271, 286
Berson J., 286
Bestvina M., 2, 47, 286
Bialynicki-Birula A., 286
Bieri R., 36, 286
Birkhoff G., 185, 191
Birman J. S., 16, 33, 34, 286
Bloh A., 286
Bochner S., 286
Bokut' L. A., 286
Borovik A., 286
Braun A., 102, 286
Brunner A. M., 41, 42, 286
Bryant R. M., 145, 286
Buchberger B., vii, 1
Burde G., 286
Burgin M. S., 284, 285
Burillo J., 286
Burns R. G., 41, 42, 286

Campbell A., 287
Campbell L. A., 71, 242, 286
Cassou-Nogues P., 284
Champagnier K., 207, 229, 234, 287
Cheng C. C., 287

Chirkov I. V., 287
Cohen M., 287
Cohn H., 287
Cohn P. M., 2, 101, 147, 193, 196, 197, 287
Comerford L. P., 8, 20, 25, 27, 42, 251, 269, 287
Connell E., 72, 75, 285, 287
Costa D., 73, 75, 287
Crowell R., 287
Czerniakiewicz A. J., 102, 138, 170, 196, 271, 288

Daigle D., 148, 156, 288
Danielewski W., 88, 91, 288
Danilov A. N., 288
Dehn M., 1
Derksen H., 288
Désarménien J., 199, 288
Dicks W., 2, 170, 177, 179, 232, 235, 244, 286, 288
tom Dieck T., 125, 288
Dobrynin N., 199, 288
Dold A., 7, 20, 42, 288
Drensky V., 2, 145, 245, 271, 286, 288, 289
Druźkowski L. M., 289
Duchamp G., 199, 288, 289
Dunwoody M. J., 235, 288
Durnev V. G., 7, 20, 21, 23, 289

Eakin P., 68, 83, 283
Eckmann B., 286, 289
Ekici N., 292
Engel E., 289
van den Essen A., 2, 3, 74, 78, 95, 96, 169, 240, 245, 284, 287–290
Evans T., 290

Feighn M., 2
Feldman G. L., 234, 290
Feng K.-Q., 290
Fiedler M., 290
Fieseler K.-H., 290
Fine B., 285, 290
Formanek E., 75, 285, 290
Fox R. H., 1, 14, 201, 287, 290
Freudenburg G., 99, 148, 156, 288, 290
Fujita T., 68, 84, 290

Gaglione A. M., 285
Gainov A. T., 205, 290
Gerasimov V. N., 290
Grätzer G., 290
Gupta C. K., 145, 271, 289, 291
Gupta N., 14, 21, 291
Gutierrez J., 289
Gwozdziewicz J., 291

Hadas O., 82, 291
Hall M., 205
Hall P., 1
Handel M., 2, 47, 286
Hedges M. C., 235, 291
Heinzer W. J., 68, 83, 283
Hill P., 21, 291

Imrich W., 291
Ivanov S. V., 21, 30, 240, 245, 291
Iyudu N. K., 291

Jacobson N., 291
Jelonek Z., 2, 70, 82, 121, 170, 240, 245, 291
Jung H. W. E., 2, 68, 72, 110, 111, 147, 150, 196, 271, 291

Kalia R. N., 292
Kaliman S., 74, 84, 122, 292
Kapovich I., 292
Karrass A., 295
Keller O., 71, 78, 138, 166, 292
Kemer A. R., 102, 292
Kharlampovich O. G., vii, 3, 235, 292
Khramtsov D. G., 46, 292
Kiral E., 292
Kolotov A. T., 292
Konieczny J., 292

Kowalski J., 293
Kraft H., 79, 293
Krasnikov A. F., 24, 293
Krob D., 199, 288, 289
Kropholler P., 23, 293
Krstic S., 2
Kryazhovskih G. V., 205, 293
Kukin G. P., 198, 205, 236, 286, 293
van der Kulk W., 2, 68, 72, 110, 111, 147, 150, 196, 271, 293
Kurosh A. G., 1, 191, 192, 293
Kutzschebauch F., 288
Kwiecinski M., 96, 289

Lam C.-M., 147, 293
Lang J., 294
Lazard M., 198, 294
Le Bruyn L., 294
Lee D., 8, 21, 30, 45, 55, 240, 245, 294
Lee W., 271
Lepowsky J., 294
Levitt G., 2, 47, 48, 294
Lewin J., 23, 192, 193, 197, 232, 288, 294
Lewin T., 294
Li W., 95, 96, 283, 294
Lichtman A. I., 294
Lin V. Ya., 109, 117, 294
Linnell P., 293
Loday J.-L., 270, 295
Logar A., 295
Loustaunau P., 284
Luengo Velasco I., 284
Lustig M., 2, 294
Lyndon R. C., 1, 3, 28, 31, 295

Müller H., 289
Magnus W., 1, 199, 235, 236, 295
Makanin G. S., 30, 295
Makar-Limanov L. G., 2, 71, 102, 124, 127, 138, 170, 196, 235, 271, 285, 295
Malcev A. I., 295
Mandelberg K., 205
Martin W. T., 286
Matsumura H., 295
McCool J., 2, 18, 46, 295
McKay J., 2, 96, 115, 295
Melançon G., 199, 288
Metzler W., 287
Mikhalev A. A., 129, 191, 198, 199, 207, 229, 231–234, 245, 246, 250, 283–285, 288, 296–298
Mikhalev A. V., 284
Miyanishi M., 68, 83, 298
Mochizuki H. Y., 285
Moh T. T., 70, 71, 73, 75, 84, 98, 108, 128, 236, 283, 298
Moody J., 293
Moser-Jauslin L., 290
Mumford D., 298
Myasnikov A. G., vii, 3, 55, 285, 286, 292, 298

Nabiyev S., 271, 285
Nagao H., 141, 143, 298
Nagata M., 147, 149, 152, 298
Neumann H., 42, 298
Neumann W., 2, 298
Nicolas J.-L., 48, 294
Nielsen J., 1, 7, 10, 20, 21, 191, 244, 298, 299

O'Neill J., 298
Oates-Williams S., 41, 42, 286
Olshanskii A. Yu., 299
Onishi H., 284
Osborne R. P., 299

Park H., 131, 135, 151, 299
Passman D. S., 299
Pedersen P., 299
Petrie T., 125, 288
Petrogradsky V. M., 199, 285, 288, 299
Pietrowski A., 18, 295

Pirashvili T., 270, 295
Plotkin B. I., vii, 3, 299
Pride S., 21, 291
Pták V., 290

Rabier P., 299
Razmyslov Yu. P., 102, 299
Reidemeister H., 1
Remeslennikov V., vii, 3, 285, 298
Reutenauer C., 231, 299
Rips E., 7, 20, 300
Rivin I., 53, 300
Rocca Jr. C. F., 32, 300
Roehl F., 285
Roman'kov V. A., 21, 300
Rosenberger G., 7, 8, 20, 35, 41, 42, 285, 290, 292, 293, 300
Rosenlicht M., 286
Rosset S., 300
van Rossum P., 295
Rowen L. H., 102, 300
Russell P., 88, 300

Sapir M. V., 292
Sathaye A., 69, 80, 81, 108, 284, 300
Schützenberger M. P., 31, 295
Scheunert M., 194, 300
Schofield A. H., 232, 300
Schreier O., 1, 191, 196, 300
Schupp P., 292, 295
Segre B., 300
Sela Z., 2
Sereguine A. V., 234, 300
Shafarevich I. R., 138, 301
Shannon D., 95, 301
Shastri A., 301
Shestakov I. P., 69, 85, 93, 206, 301
Shevelin M. A., 287
Shirshov A. I., 1, 191, 235, 301
Shirvani M., 294
Shpilrain V., 7, 8, 17, 20, 21, 35, 55, 71, 150, 169, 170, 207, 208, 229, 231, 232, 234, 239, 240, 242, 244, 245, 247, 250, 269, 271, 285, 286, 289–292, 295, 296, 298, 301, 302
Shtern A. S., 191, 302
Sims C., 46, 55
Singh B., 110, 284
Slinko A. M., 301
Smith M. K., 94, 99, 103, 148, 163, 164, 168, 302
Solitar D., 295
Spellman D., 285, 290
Srinivas V., 302
Stallings J. R., 2, 8, 35, 42, 233, 302
Stefanov D., 288
Stille M., 290
Sturmfels B., 295, 299, 303
Sugie T., 68, 298
Suslin A. A., 36, 132, 138, 247, 303
Suzuki M., 108, 303
Swan R. G., 233, 303
Sweedler M., 95, 301

Tietze H., 1, 13
Timoshenko E. I., 22, 32, 291, 303
Turner E. C., 2, 7, 20, 21, 25, 32, 42, 244, 291, 298, 300, 303
Tutaj H., 78, 290

Ufnarovskii V. A., 303
Umirbaev U. U., 16, 35–37, 69, 85, 93, 95, 103–105, 107, 130, 191, 202, 205, 206, 208, 229, 231, 233, 235, 245, 246, 283, 296, 297, 301, 303, 304

Vasilieva E. A., 304
Ventura E., 2, 286
Viennot G., 304
Voce D., 27, 304

Vogtmann K., 2

Wang S. S., 2, 72, 96, 115, 287, 295, 304
Wasserman A., 300
Weinbaum C. M., 304
Whitehead J. H. C., 1, 12, 53, 109, 111, 129, 235, 304
Wightwick P., 2, 87, 111, 298, 304
Wilson R. J., 304
Wilson R. L., 294
Winkelmann J., 288
Witt E., 1, 191, 304
Wolny J., 292, 293
Woodburn C., 299
Wright D., 2, 72, 131, 137, 147, 150, 154, 158, 164, 285, 304

Yagzhev A. V., 231, 304
Yu J.-T., 71, 93, 96, 147, 148, 150, 208, 234, 242, 245, 246, 287, 289, 290, 293–297, 302–305

Zaicev M. V., 191, 285, 305
Zaidenberg M. G., 109, 117, 292, 294, 305
Zhevlakov K. A., 301
Zhukov A. I., 235, 305
Zieschang H., 7, 20, 39, 179, 286, 299, 305
Zimmermann B., 287
Zolotykh A. A., 129, 194, 207, 229, 231–234, 245, 250, 296–298, 305
Zweibel J., 75, 287

Subject Index

$\mathfrak{A}$-generic element, 264
"abridged" automorphic orbit, 48
"abridged" orbit, 45
admissible set, 217
Akivis algebra, 206
Alexander matrix, 119
algebraic variety, 80, 108
algorithm for recognizing test elements, 27
almost primitive element, 8, 41, 246, 256
APE, 41, 44, 246
augmentation ideal, 14, 36
augmentation-preserving automorphism, 139
automorphic conjugacy problem, 11
automorphic orbit, 8, 45, 59

bicharacter, 194

C-test word, 31, 32
cancellation conjecture, 68, 80
chain rule, 15, 132
color Lie p-superalgebra, 195
color Lie superalgebra, 194
commutation factor, 194
commutator test, 17, 21, 139
coordinate polynomial, 69, 72, 129, 149, 170
cut vertex, 49
cyclically reduced primitive element, 52
cylinder, 81
cylindrical hypersurface, 81

degree, 192
Δ-primitive element, 8, 35, 36, 247, 262
density of coordinates, 144
double Jacobian matrix, 33, 37

elementary automorphism, 68, 192
elementary ideal, 120
elementary reducible element, 280
elementary regular transformation, 28

elementary singular transformation, 28
elementary transformation, 112, 125, 130, 133, 192
elimination of variables, 198
elimination theorem, 199
embedding conjecture, 69, 108, 127
embedding problem, 108
equivalent algebraic varieties, 108
even element, 194

(f, g)-uncancellable system, 277
face polynomial, 96, 115
finite automorphic orbit, 46
Fox derivation, 33
Fox derivative, 14, 141, 144
Fox gradient, 15, 18, 127
Fox partial derivation, 201
free abelian extension in a variety, 206
free algebra, 185
free anticommutative nonassociative algebra, 194
free associative algebra, 127, 138, 155, 169
free color Lie p-superalgebra, 195
free color Lie superalgebra, 195
free commutative nonassociative algebra, 193
free group ring, 35
free Leibniz algebra, 271
free nonassociative algebra, 193
free special Jordan algebra, 139
Freiheitssatz, 127, 235
functional, 217

G-graded Lie algebra, 195
G-graded set, 195
generalized degree function, 192
generic element, 8, 41, 43
generic polynomial, 82, 170
Gröbner basis, 95
Gröbner reduction, 131

holomorphic automorphism, 126
homogeneous variety of algebras, 185
hyperplane, 81
hypersurface, 81

IA-automorphism, 21
identity, 185
IL-automorphism, 139
independent subset, 192
inverse function theorem, 16, 33

Jacobian conjecture, 67, 71, 137
Jacobian matrix, 220, 231

leading part, 192
Leibniz algebra, 270
locally nilpotent derivation, 103, 156

m-homogeneous element, 217
M-test word, 30
μ-bounded element, 225
μ-degree, 217
μ-homogeneous element, 217
μ-homogeneous endomorphism, 219
multidegree, 217

Nagata automorphism, 98, 104, 148, 154, 159, 172
Nagata's problem, 68, 92
Newton polygon, 77, 110, 115
Newton polytope, 82
Nielsen equivalent sets, 10
Nielsen property, 192
Nielsen-reduced set, 10
Nielsen transformation, 10
number of primitive elements, 48, 52

odd element, 195
outer rank, 129, 169

parametric curve, 111, 113
partial derivative, 202
PBW type theorem, 203
peak reduction, 12, 109, 112
polynomial parametrization, 109
primitive element, 8, 45, 127, 139, 170, 208
primitive system of elements, 208
property of differential separability for subalgebras, 202

rank, 25, 60, 208, 211
rank of a system of elements, 225
rank of an element, 225
reduced Gröbner basis, 96
reduced subset, 192
relation module, 15
residually finite algebra, 204, 271
restricted universal enveloping algebra, 202
resultant, 115
retract, 25, 72, 76, 242, 245
retraction, 25, 72
retraction homomorphism, 245

Schreier property, 192
Schreier variety of algebras, 185
Schreier's formula, 197
simple automorphism, 280
skew symmetric bilinear form, 194
stable equivalence conjecture, 81
stable image, 26, 75
stably equivalent algebraic varieties, 119
stably equivalent polynomials, 81
stably equivalent systems, 209
stably tame automorphism, 164, 168

T-ideal, 102
"tag" monomial ordering, 95
"tag" variable, 95
tame APE, 41
tame automorphism, 68, 92
tame coordinate, 149
test element, 7, 20, 25, 169, 175, 244
test polynomial, 70, 82, 169
test rank, 32
test set, 30, 32
Tietze transformation, 14, 18, 117, 128
triangular automorphism, 92, 149
triangular derivation, 162

$\mathfrak{U}$-generic element, 246, 247
unimodular gradient, 131, 148, 156
universal derivation, 202
universal derivation of $L(X)$, 206
universal derivation of $K\langle X\rangle$, 232
universal enveloping algebra, 202
universal multiplicative enveloping algebra, 193
universal operators of left and right multiplication, 193

variety, 185

weak algorithm, 197
Whitehead automorphism, 28, 53, 59
Whitehead graph, 28, 49, 60
Whitehead transformation, 12
Whitehead tree, 50
Whitehead's algorithm, 53, 55
wild automorphism, 92, 158
wild coordinate, 151

$\mathbb{Z}F$-primitive element, 36